Advanced Engineering Informatics xxx (2016) xxx–xxx

Contents lists available at ScienceDirect

Advanced Engineering Informatics

journal homepage: www.elsevier.com/locate/aei

Review article

A review of essential standards and patent landscapes for the Internet of Things: A key enabler for Industry 4.0

Amy J.C. Trappey [a,*], Charles V. Trappey [b], Usharani Hareesh Govindarajan [a], Allen C. Chuang [a], John J. Sun [a]

[a] *Department of Industrial Engineering and Engineering Management, National Tsing Hua University, Hsinchu, Taiwan*
[b] *Department of Management Science, National Chiao Tung University, Hsinchu, Taiwan*

A R T I C L E I N F O

Article history:
Received 5 June 2016
Received in revised form 24 October 2016
Accepted 29 November 2016
Available online xxxx

Keywords:
Industry 4.0
Internet of Thing (IoT)
Patent analysis
Cyber-physical systems (CPS)
Technology standards

A B S T R A C T

This paper is a formal overview of standards and patents for Internet of Things (IoT) as a key enabler for the next generation advanced manufacturing, referred as Industry 4.0 (I 4.0). IoT at the fundamental level is a means of connecting physical objects to the Internet as a ubiquitous network that enables objects to collect and exchange information. The manufacturing industry is seeking versatile manufacturing service provisions to overcome shortened product life cycles, increased labor costs, and fluctuating customer needs for competitive marketplaces. This paper depicts a systematic approach to review IoT technology standards and patents. The thorough analysis and overview include the essential standard landscape and the patent landscape based on the governing standards organizations for America, Europe and China where most global manufacturing bases are located. The literature of emerging IoT standards from the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC) and the Guobiao standards (GB), and global patents issued in US, Europe, China and World Intellectual Property Organization (WIPO) are systematically presented in this study.

Contents

* Corresponding author.
E-mail address: trappey@ie.nthu.edu.tw (A.J.C. Trappey).

http://dx.doi.org/10.1016/j.aei.2016.11.007
1474-0346/

Please cite this article in press as: A.J.C. Trappey et al., A review of essential standards and patent landscapes for the Internet of Things: A key enabler for Industry 4.0, Adv. Eng. Informat. (2016), http://dx.doi.org/10.1016/j.aei.2016.11.007

Nomenclature

AIDC	Automatic Identification and Data Capture
CPS	Cyber-Physical Systems
EPO	European Patent Office
ETSI	European Telecommunications Standards Institute
GB	Guobiao standards (Standardization Administration of China)
GB/T	Guobiao standards recommended
GB/Z	Guobiao standards guide
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Intellectual Property
IPC	International Patent Classification
ISO	International Organization for Standardization
I 4.0	Industry 4.0
RFID	Radio Frequency Identification
TI	Thomson Innovation
UKIPO	United Kingdom Intellectual Property Office
US	United States
USPTO	United States Patent and Trademark Office
WIPO	World Intellectual Property Organization
WWW	World Wide Web Consortium

1. Introduction

Intelligence is the key enabler to facilitate work and in a broad sense and consists of two parts. Algorithmic intelligence describes how to reach a goal via a process (e.g., driving your car to a destination) and tactical intelligence describes how to reach the destination with consideration to changing factors (e.g. checking the car tire pressure to compensate for changing road conditions). I 4.0 in the simplest form concerns enabling manufacturing with the element of tactical intelligence using techniques and technologies such as IoT, cloud computing and big data. IoT is considered to be a paradigm shift for Internet technologies. Estimations show that as of 2014 the number of IoT-enabled devices has exceeded the world's human population. IoT is used by consumers as well as by manufacturers that rely on cyber (software, data systems) and physical (devices, machinery, equipment) connectivity to function effectively. While I 4.0 was initially considered a technology experiment, it is now a necessity to maintain competitiveness in a constantly changing industry environment. IoT is a core enabling technology that enables industries to move from I 3.0 to I 4.0 by inserting intelligence into products and processes across the supply chain. I 4.0 also represents the aggregation of IoT, CPS, cloud computing and big data analytics to improve the goal of a near zero defect state [1] (see Fig. 1).

This article intends to present the latest development overviews in the field of Internet of Things (IoT) as a key enabler for Industry 4.0 (I 4.0). The main emphases include

- The formal background and introduction to I 4.0 and IoT are described using a layering of IoT device and process terms. For the sake of clarity, IoT technologies are separated into four layers that are organized to consolidate the focus of IoT innovations consistent with the literature and emerging standards for advanced manufacturing.

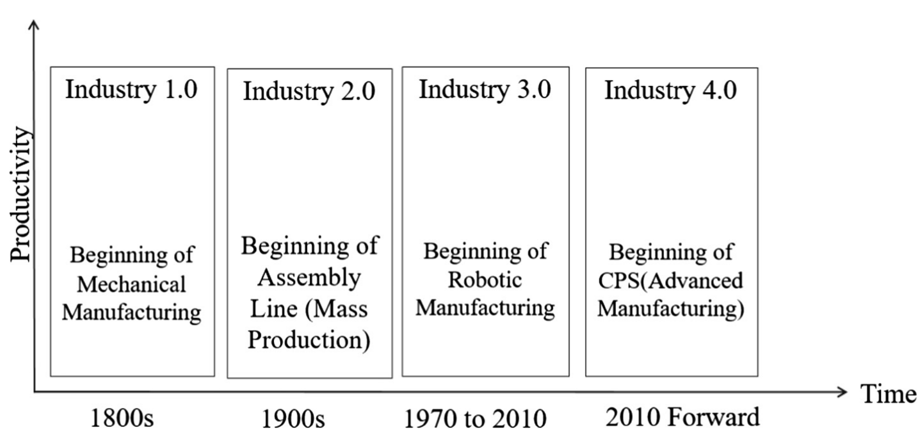

Fig. 1. Industry evolution graph [2].

Please cite this article in press as: A.J.C. Trappey et al., A review of essential standards and patent landscapes for the Internet of Things: A key enabler for Industry 4.0, Adv. Eng. Informat. (2016), http://dx.doi.org/10.1016/j.aei.2016.11.007

- The analysis and consolidation of I 4.0 context standards landscape for IoT are constructed with information abstracted from official/governing bodies, such as the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), and the Guobiao standards (Standardization Administration of China GB).
- The analysis and creation of a patent landscape for IoT in the I 4.0 context using information abstracted from the World Intellectual Property Organization (WIPO) and United States Patent and Trademark Office (USPTO).

The significance of this research is to understand the emerging standardization landscape and the technical impact of the IoT related patents. The trends and outcomes will identify the potential creation of patent barriers, the exploration of new technologies for long-term commercialization, and strategies that may be adapted to accelerate the adoption of IoT technologies. The research provides academicians and practitioners with a scientific basis to predict future development trends and evaluate the status of their IoT technology infrastructure.

1.1. Motivation

The motivation for this paper comes from the need to understand the nature and causes of the collaborative trends of industries to standardize and license technologies. The rapid pace of collaboration leads to the creation and adoption of many technologies and ultimately shorter product life cycles. Industries that collaborate harness the potential of rapid change and realize new market benefits. Standardization helps industry avoid interoperability issues and understand the technology landscape as the new technology frontier is created.

2. Background and literature review of IoT

The phrase Internet of Things (IoT) was first used by Ashton in 1999 [3]. The concept of IoT is to enable real world objects with speech, vision, hearing, smell, and touch, so inanimate things can perform jobs more accurately and responsively collaboratively and with learning [4–7]. The transformation is possible only when sets of technologies are created that are broadly applicable to industry. Various aspects of IoT technology have been reviewed in the academic literature [4–18] and may be referenced as cited for a detailed literature review of IoT technologies. IoT layering is one of the classification methods used to establish a logical framework to categorize and identify CPS. Thus, this paper uses layers to define technology categories and components as the framework to position the essential standard and patent landscapes of the Internet of Things.

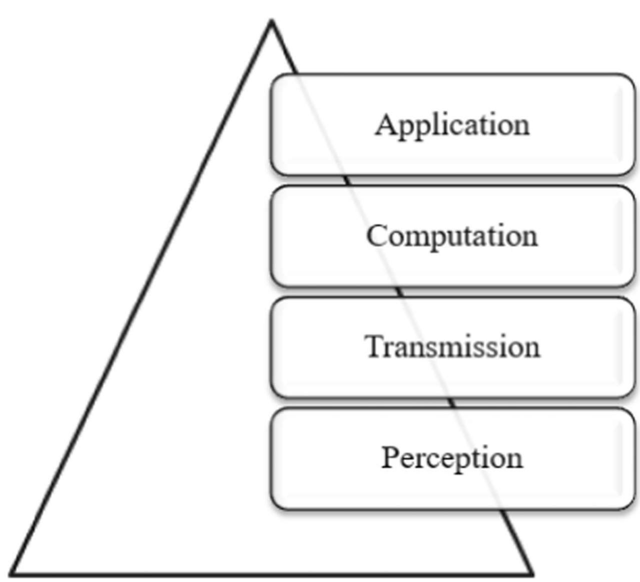

Fig. 2. IoT layers.

There are many numbers of layers reviewed in the literature (from five to nine layers) [4–5,18–23]. After the evaluation of the existing literature, the most appropriate layer and best suited to industrial application divides the IoT architecture into four layers (see Fig. 2). Components in the IoT architecture are logically and intuitively placed under the perception, transmission, computation and application layers [4–14]. A detailed explanation of the layers is provided in the following sections.

2.1. Perception layer

Perception deals with the types of sensors and actuators that help the physical object to perceive. Perception is used in upper layers to achieve the final goal of micro intelligence at the application layer. A sensor is a device that sends an output by detecting changes in quantities, qualities, or events. The goal of the perception layer is to enable objects with a sense of vision, touch, smell, hearing, and thinking [9,24]. Some commonly used sensors in the IoT ecosystem are used to detect temperature, weight, motion, vibration, acceleration, humidity, and location [18] (see Fig. 3).

2.2. Transmission layer

Transmission is the second layer in the IoT ecosystem. The next step after perception (collection of sensor information) is to transmit the information to the upper layers. Transmission is limited by factors such as power, range and storage capacity (most IoTs operate on low power with a short range). There is an emerging set of technologies, architectures, and infrastructures that are being standardized with these considerations in mind. Some prominent transmission technologies and protocols are listed below (see Fig. 4).

2.3. Computation layer

The computation layer describes means of receiving data, processing data, making decisions and delivering the decisions to the application layer. The computation layer consists of hardware, software, algorithms, cloud computing, big data analysis and security (see Fig. 5).

2.4. Application layer

The application layer provides tactical understanding by using information collected and transmitted from lower layers. The application layer consists of consumer (IoT2C) and business (IoT2B) categories as described below (see Fig. 6).

3. Standards for IoT

Standards simplify the job of stakeholders by ensuring uniformity and encouraging interoperability. With the introduction of I 4.0, many countries have actively developed and promoted the new industry standard. Equipment, suppliers, factories, production lines, products and customers are integrated under I 4.0. Therefore, there are specific standards for all players. Fig. 7 shows the standard structure of I 4.0 which consists of two parts, the basic common standards and the key technology standards [25].

Please cite this article in press as: A.J.C. Trappey et al., A review of essential standards and patent landscapes for the Internet of Things: A key enabler for Industry 4.0, Adv. Eng. Informat. (2016), http://dx.doi.org/10.1016/j.aei.2016.11.007

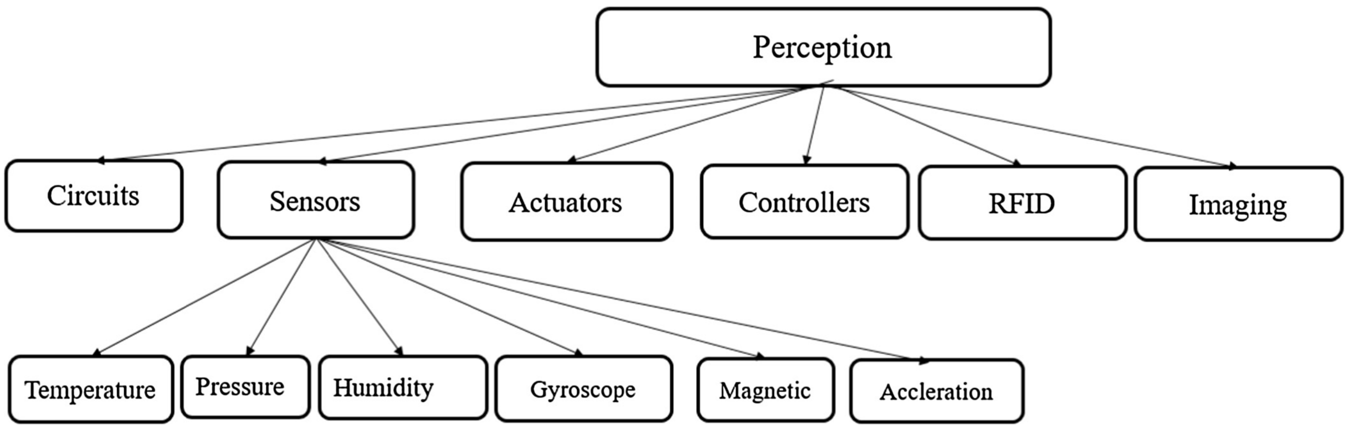

Fig. 3. IoT perception layer classification.

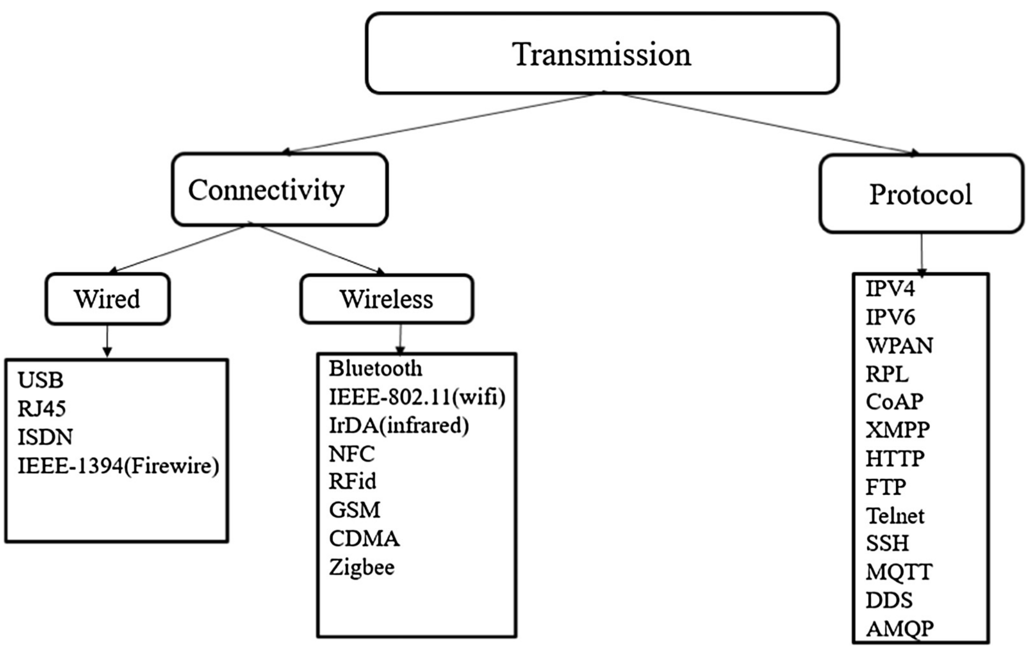

Fig. 4. IoT transmission layer classification [9].

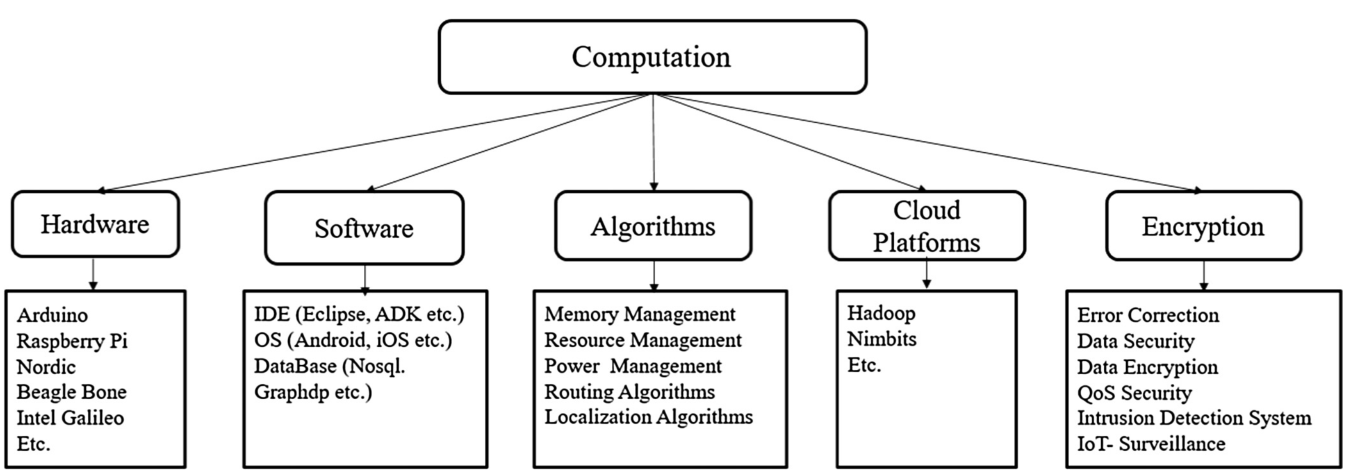

Fig. 5. IoT computation layer classification [18].

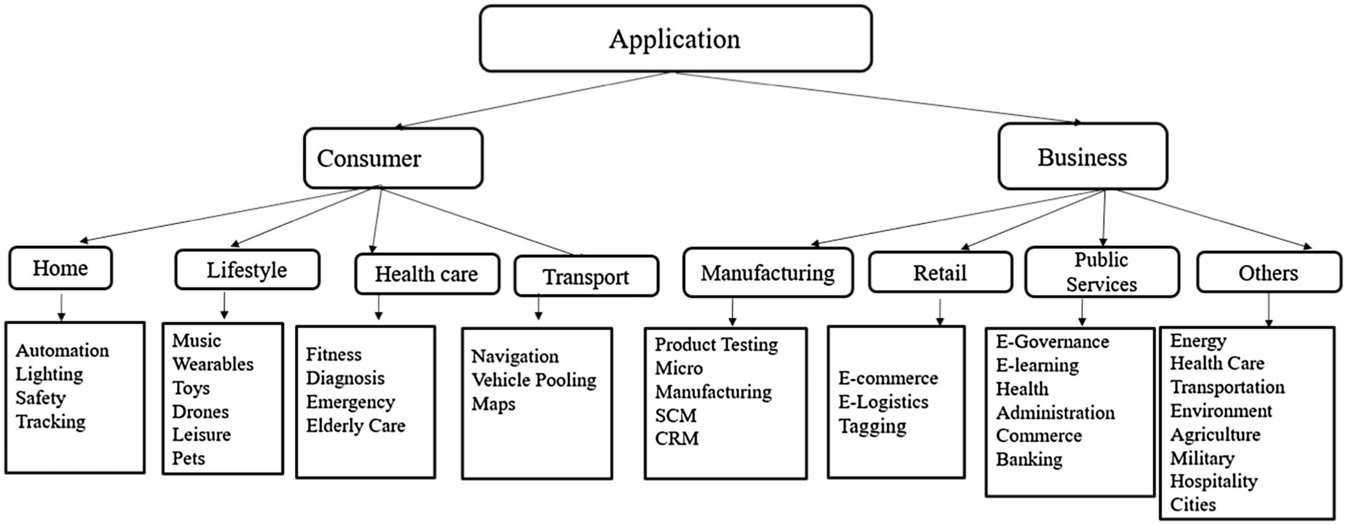

Fig. 6. IoT application landscape [7].

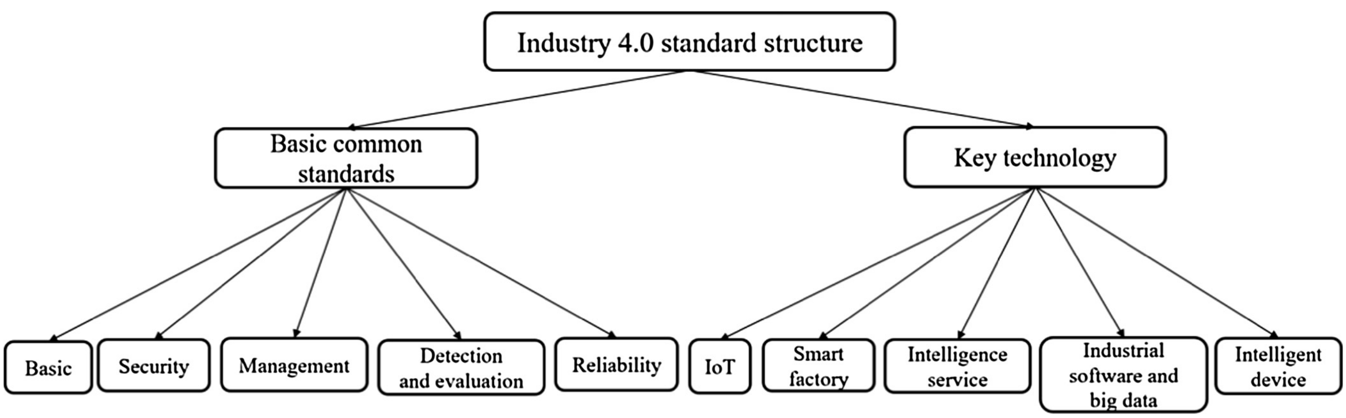

Fig. 7. I 4.0 standard structure [25].

3.1. Standard bodies

The standardization bodies such as IETF, IEEE and ETSI are critical to the technology development of IoT [26]. The technical specifications defined by consensus are recognized by the industry as the accepted standards. This study focuses on IoT standards, which takes industry technical specifications into consideration and have been officially issued by the ISO and IEC after completing the international standardization processes.

3.1.1. International Electrotechnical Commission (IEC)

The IEC was established in 1906 and is the oldest international organization for Electrotechnical Standardization. The IEC is responsible for the international standardization in the field of electrical engineering and electronic engineering. IEC's Standardization Management Board (SMB) and is the agency covers the overall management of the IEC technical specifications and standardization. SMB is responsible for strategic planning, adjustment, execution and supervision of the activities of the Technical Committee. IEC/SMB/SG8 is the strategic working group for smart manufacturing technologies and is responsible for developing I 4.0 relevant and key technical standards. The results of IEC/TC65 are the technical committee core to the international standardization of I 4.0 since IEC/TC65 focuses on industrial processes, measurement, control and automation [27].

3.1.2. International Organization for standardization (ISO)

The ISO was established in 1947. ISO is an independent organization and non-government international organization with 162 global members. The organization brings experts together to share knowledge and develop international standards. The ISO works closely with the IEC on the development of I 4.0 standards. ISO/TC 184 is important to the international standardization of I 4.0 and focuses on automation systems and integration [28].

3.1.3. ISO/IEC JTC 1

ISO/IEC JTC1 has established the Working Group (WG) 10 for the Internet of Things. ISO/IEC JTC 1 is the standards development environment where experts come together to develop worldwide Information and Communication Technologies (ICT) standards. ISO/IEC JTC1/WG 10 serves as a focus group for IoT standardization program. The official objectives of ISO/IEC JTC1/WG 10 are [29]:

- Develop terms and definitions for JTC 1 IoT vocabulary.
- Develop an IoT reference architecture and other fundamental specifications such as JTC 1 standards.
- Continuing the work of in SWG on IoT concerning standardization gaps.
- Establishing a liaison with JTC 1, ISO, IEC or other committees or working groups undertaking work related to IoT.

Please cite this article in press as: A.J.C. Trappey et al., A review of essential standards and patent landscapes for the Internet of Things: A key enabler for Industry 4.0, Adv. Eng. Informat. (2016), http://dx.doi.org/10.1016/j.aei.2016.11.007

- Encouraging the prompt and efficient exchange of information within JTC 1 and with ISO, IEC, or other committees or working groups working on IoT.
- Monitoring ongoing IoT regulations, markets, businesses, and technology requirements.
- Develop IoT standards that build on the foundation standards and use relevant JTC 1 subgroups for further development.

There are other IoT related working groups including ISO/IEC JTC 1/WG 7 for sensor networks and ISO/IEC JTC 1/SC 31 for automatic identification and data capture techniques [29,30].

3.2. The IoT standard structure

This section maps the IoT ISO/IEC standards landscape to the four-layered architecture explained in Section 2. The corresponding Chinese standards (GB) are also depicted in Fig. 8 [25–91] and Appendix A. The highlights of the standardized technical specifications are shown in Fig. 9 [18,92].

3.3. Perception layer standards

The perception layer concerns utilizing sensors to obtain data and information occurring in the physical world. In addition, data collection depends on technologies such as sensors, RFID, two-dimensional codes, and real-time location technology. There are also sensor data exchange standards including TransducerML, SensorML, IRIG, CBRN, EXDL and TEDS [92]. These standards focus on the definitions from ISO/IEC for AIDC methods including sensors and RFID. AIDC is a global application and is an important part for IoT. If information is needed at any time, then AIDC technology is required. ISO and IEC have developed many standards in this field. ISO/IEC 19762:2016 provides terms and definitions for automatic identification techniques [66].

The following descriptions are the relevant standards for RFID. The ISO/IEC 15459 series defines the unique identification for registration procedures, common rules, individual transport units, individual products and product packages, individual returnable transport items, and groupings [71]. The ISO/IEC 15963-2009 describes numbering systems that are available for the identification of RFID tags [72]. The ISO/IEC 18000 series provides definitions for different unique frequency ranges for diverse RFID technologies so that users can choose suitable types of devices according to demand [78]. The ISO 6346:1995, ISO/TS 10891:2009, ISO 10374:1991, ISO 18185 series provides definitions for coding, communication, and application of RFID electronic seals for freight containers. These methods ensure that the RFID tag attached to the container can operate in a variety of environments. These standards are important for the integration of the supply chain information. The ISO 17363:2013, ISO 17364:2013, ISO 17365:2013, ISO 17366:2013, ISO 17367:2013 standards are relevant to RFID applications related to supply chain management. These standards define the technical aspects and data hierarchy for information required at each layer of the supply chain [73–77]. The ISO/IEC 29143:2011, ISO/IEC TR 29172:2011, ISO/IEC 29173-1:2012, ISO/IEC 29175:2012, ISO/IEC 29176:2011, ISO/IEC 29178:2012, ISO/IEC 29179:2012 standards include mobile AIDC and mobile RFID related standards which enable flexibility to capture data [80–86].

Some standards are designed for smart sensors and sensor networks. The ISO/IEC 29182 series provides a Sensor Network Reference Architecture (SNRA) that helps users to develop sensor networks [61]. The ISO/IEC 20005:2013, ISO/IEC 30101:2014, ISO/IEC 30128:2014, ISO/IEC/IEEE 21450:2010, ISO/IEC/IEEE 21451 standards are used to create intelligent sensor networks. The topics covered by these standards include collaborative information processing, smart grid systems, and smart transducer interfaces. By applying the above standards, users can build more reliable and intelligent sensor networks [67–69,88–89].

3.4. Transmission layer standards

The transmission layer transmits information from the perception layer to the application layer through the base bearer network. There are some wired communication standards for the technology, such as IP, Everything over IP: Ethernet, ATM, Frame Relay, SDH, FDDI, Fiber Channel, ISDN, VPN, VoIP, Cable/xDSL, BACNet, CanBus, ControlNet, DeviceNet, Dupline, FF, HART, InterBus, LonWorks, ModBus, ProfiBus, SwiftNet, Vnet/IP, WorldFIP, CC-Link,

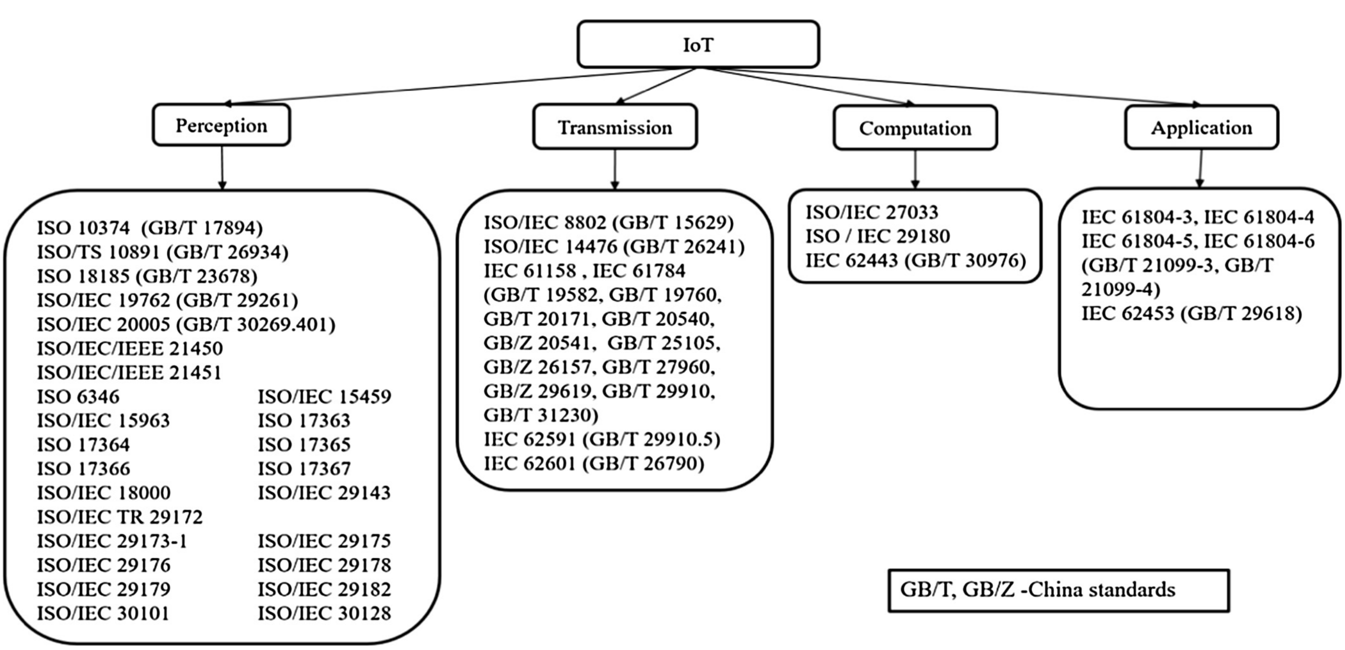

Fig. 8. IoT standard structure [25–91].

Please cite this article in press as: A.J.C. Trappey et al., A review of essential standards and patent landscapes for the Internet of Things: A key enabler for Industry 4.0, Adv. Eng. Informat. (2016), http://dx.doi.org/10.1016/j.aei.2016.11.007

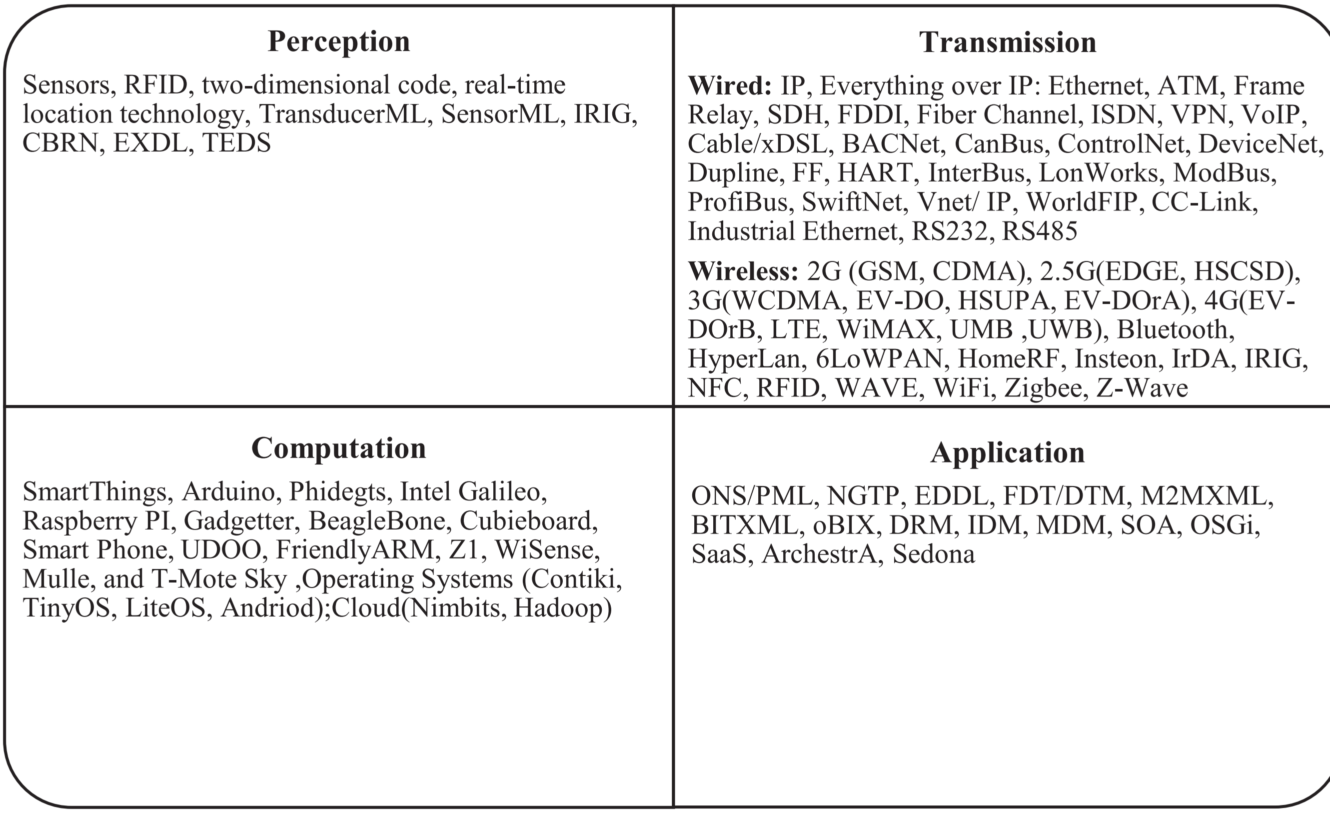

Fig. 9. The highlights of the standardized technical specifications [18,92].

Industrial Ethernet, RS232, and RS485. There are also wireless standards, such as 2G (GSM, CDMA), 2.5G (EDGE, HSCSD), 3G (WCDMA, EV-DO, HSUPA, EV-DOrA), 4G (EV-DOrB, LTE, WiMAX, UMB, UWB), Bluetooth, HyperLan, 6LoWPAN, HomeRF, Insteon, IrDA, IRIG, NFC, RFID, WAVE, WiFi, Zigbee, and Z-Wave [92]. There are wired or wireless communication protocols for the transmission layer. The following references link international standards related to the transmission layer of IoT which include the ISO/IEC 8802 series for local area networks (LAN) and metropolitan area networks (MAN). LAN is used for a small range of wired or wireless transmissions used in small workplaces, homes, and offices. MAN is connected to a number of LANs and both standards belong to small-scale communications [62].

There are standards for wired communications. The IEC 61158 series and IEC 61784 series are standards for fieldbus configurations and profiles including Foundation Fieldbus, Common Industrial Protocol, PROFIBUS and PROFINET, P-Net, WorldFIP, INTERBUS, SwiftNet, CC-Link, HART, VNET/IP, TCnet, EtherCAT, Ethernet POWERLINK, Ethernet for Plant Automation (EPA), Modbus, SERCOS, RAPIEnet, SafetyNet p and MECHATROLINK. The above protocols are used for real-time distributed control [53–54].

There are several standards for wireless transmission including the IEC 62591:2016 (Wireless HART™) and IEC 62601:2015 (WIA-PA). WIA-PA is an industrial wireless communication standard for process automation and is suitable for industrial measurement and monitoring of wireless network systems. Wireless HART™ is a standard specifically designed for process measurement and control applications for managing real-time operations. Both are used in industrial wireless transmission and the ISO/IEC 14476 series is used to enhance the communications transport protocol and ensure the Quality of Service (QoS) [58–60].

3.5. Computation layer standards

Computation includes algorithms needed to create or transform transmitted and collected data. There are some topics in the computing layer that contain routing algorithms, image processing, character recognition, error correction, data security, and data encryption. In addition, there are some hardware technologies related to the computation layer including SmartThings, Arduino, Phidegts, Intel Galileo, Raspberry PI, Gadgetter, BeagleBone, Cubieboard, Smart Phone, UDOO, FriendlyARM, Z1, WiSense, Mulle, and T-Mote Sky. These hardware technologies were developed to run IoT applications. There are also software technologies including Operating Systems (Contiki, TinyOS, LiteOS, Andriod) and Cloud applications (Nimbits, Hadoop) [18]. These software technologies are utilized to increase IoT functions. The following lists standards for data security and system security.

There are three standards for the security of the sensors, networks and control systems. The ISO/IEC 29180:2012 is used to ensure the security for ubiquitous sensor networks [87]. The ISO/IEC 27033 series is used to ensure the security of network and information and reduces the risk of an information security crisis [79]. The IEC 62443 series ensures the security of industrial automation and control systems and provides comprehensive security protection [56].

3.6. Application layer standards

The application layer uses the collected data to form a dynamic data resource base which is suitable for the IoT related business requirements. The IoT related businesses including retail, health, energy, mobility, cities, manufacturing, publishing, and services. The application layer the categories data standards and software frameworks. The data standards contain ONS (Object Name

Service)/Physical Markup Language (PML), Next-Generation Telematics Protocol (NGTP), Electronic Device Description Language (EDDL), FDT/DTM, OPC, M2MXML, BITXML, and Open Building Information Xchange (oBIX). Included are software frameworks such as DRM, IDM, MDM, SOA, OSGi, Software as a Service (SaaS), ArchestrA, and Sedona [92]. The following lists some IEC international standards related to the application layer of IoT.

The IEC 62453(FDT) is used for the standardization of communication and configuration interfaces between field equipment and host systems. Equipment can be configured, operated, and maintained through the user interfaces [57,93]. The IEC 61804-3, the IEC 61804-4, the IEC 61804-5, and the IEC 61804-6 (EDDL) are used to describe the digital communication characteristics of intelligent field instrumentation and equipment parameters. The EDDL technology enables host system manufacturers to create a single engineering environment that supports a variety of equipment, from any supplier, and is a communication protocol [55,94].

3.7. How to use standards

Companies implementing IoT consider established standards based on common terminologies. The IEC 61360, the IEC 61987, the IEC 62683 (Common Data Dictionary), are three standards that include the related terminology of IoT. The standards mapped to the perception layer are used to build sensors, RFID systems, and AIDC facilities. The equipment interoperability standards are key to IoT implementation. The IEC 61804 (EDDL) and the IEC 62453 (FDT) increase the interoperability between machines. Communication is critical for IoT implementation. The standards in the transmission layer such as the IEC 62591 (WirelessHART) and the IEC 62601 (WIA-PA) build open communication networks. Given a transmission platform, the security information must be protected. The IEC 62443 and the ISO 27033 series define information security. The relevant installation and construction of these features are described by IEC 62794 and IEC 62832 that provides reference models for companies to build a digital factory [25–26,91,95].

4. IoT patents related to manufacturing applications

Standard essential patents (SEPs) and the related emerging standards are mapped to the intellectual property owners to better understand the leaders defining the technology landscape. For example, on September 10, 2015, Ericsson invited other companies to participate in a joint licensing program for standard essential patents indicating the creation of a standard patent pool in the near future [96]. In order to predict which companies will develop patent joint licensing agreements, a patent portfolio analysis is conducted. Based on the former section, the Internet of Things (IoT) is divided into four layers, i.e. the perception layer, the transmission layer, the computation layer, and the application layer. There are many keywords with respect to these corresponding technologies. The first part of the methodology identifies the keywords for searching documents and for creating the ontologies of IoT technologies mapped to corresponding layers.

4.1. Patent search strategy

The patent portfolios are organized using the TI patent search system. The patents are searched from January 1st 2006 to December 31st 2015. The prior research about IoT patent landscapes conducted by the UKIPO selected the top five regions by number of patents which are China, the US, Japan, Korea and the WIPO. The search included France and EPO patents [97]. The scope of patents searched in this study include granted patents in the US, Europe, China, Japan, Korea, France and WIPO. WIPO is the abbreviation of World Intellectual Property Organization, which is responsible for the intellectual property protection under the United Nations. Patents applied for under the WIPO may have higher values than country-specific applications. These patent applicants use the international patent cooperation treaty (PCT). Patents granted under PCT could receive patent protection across several countries using a simplified process of simultaneous global patent applications [98]. EPO is the abbreviation of European Patent Office, which is in charge of the patent protection in Europe. Patent applicants can apply for European patents under the European Patent Convention (EPC) designating one or multiple EPC member countries for the patent applications. The WIPO and the EPO are significant agencies managing the applications for international patents [99]. The France Patent Office, like other national patent offices, only handles patent applications under the jurisdiction of its own country [100]. The patent offices in China, the US, Japan, and Korea are referred to as SIPO, USPTO, JPO, and KIPO, respectively.

Table B1 in Appendix B explains keywords from the literature for each layer of the IoT. This research constructs the ontology of IoT using the keywords that match each layer of the IoT [Appendix B]. The research builds the patent portfolio by using keywords from the ontology that correspond to the four sub-fields of IoT. The flowchart for searching the patents is shown below. Please refer to Fig. 10 for details describing the flowchart process. The research utilizes all keywords which correspond to the layers of IoT. In order to specify how the search terms are organized, Fig. 11 provides functions and the relationships. The patent analysis section is divided into two parts to include a management perspective and a technology analysis perspective. The management perspective applies graph and patent maps to depict trends and opportunities. The technology analysis uses a technology application matrix. The matrix is created by constructing the technology columns based on key IoT technologies from the Internet of Things (IoT) patent landscape analysis written by LexInnova. The application columns are created by referring to IoT-related papers which focus on manufacturing industry applications. The technology application matrix provides a detailed numerical analysis for research and development personnel to study and predict patent trends of the future.

4.2. IoT ontology layers

An ontology is a tool that is defined as a formal, explicit specification of a shared conceptualization and can be used to represent knowledge details within a domain as a set of concepts and their relationships. An ontology has four components: classes, relations, attributes and individuals. The structure enables researchers to understand the complete set of knowledge concepts as objects and their relationships between objects [19].

The related technologies in the perception layer are centered about the infrastructures of IoT and include sensors, circuits, actuators, controllers, cameras, printed circuit boards (PCB), and RFID. Sensors are divided into several main application categories, including temperature, humidity, buttons, compasses, light detection, and current meters. Please refer to Fig. 12 for detailed definitions of the perception layer ontology [5,24].

The related technologies in the transmission layer define the networking of IoT, including topology management, multiplexing methods, communication protocols, radio frequency protocols, baseband processing, data aggregation/processing protocols, data storage/retrieval protocols, business model protocols, business application protocols, link layer protocols, connectivity protocols, and transport protocols. Please refer to Fig. 13 for detailed definitions of the transmission layer ontology [9,24].

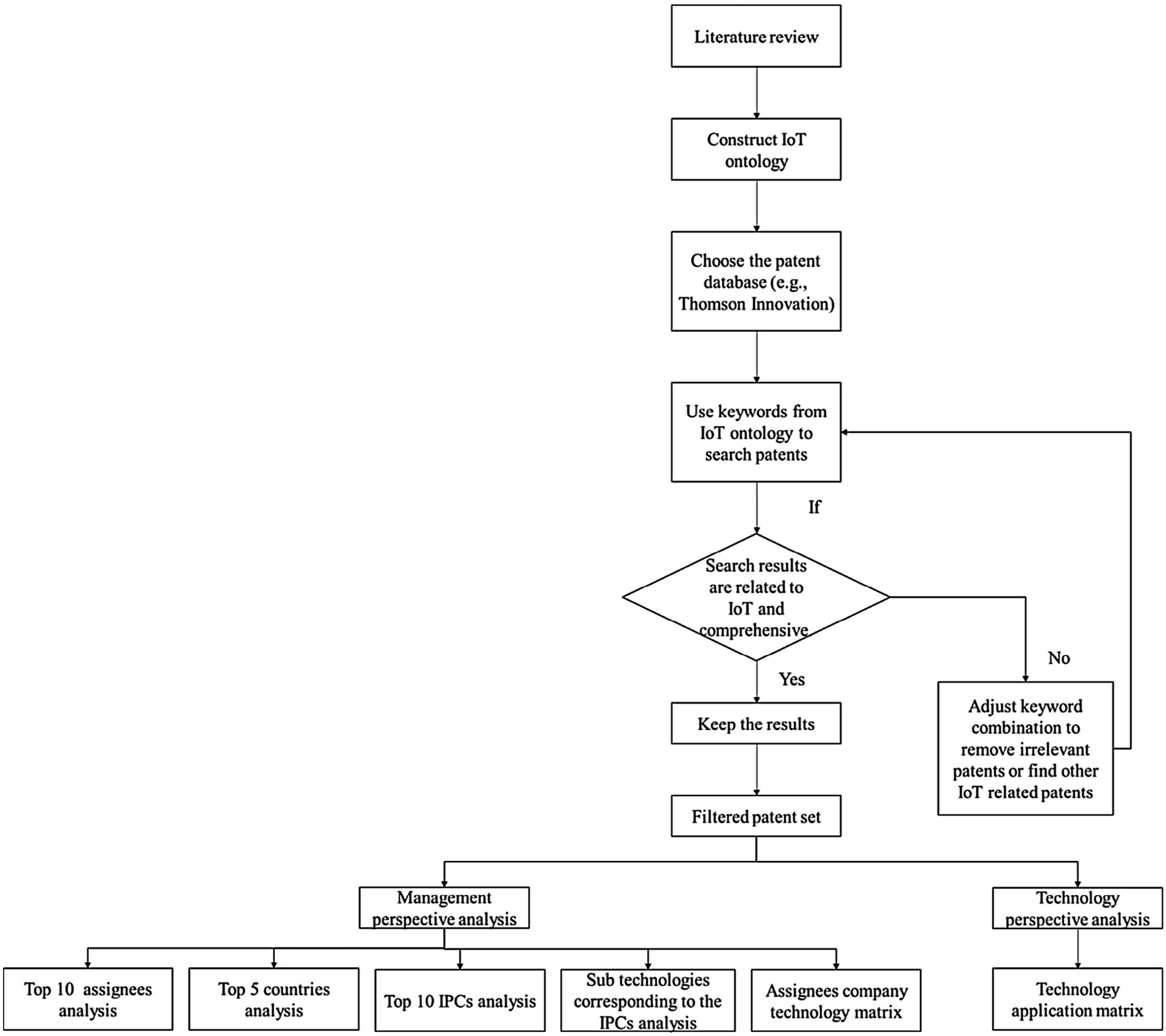

Fig. 10. Flowchart for searching the patents.

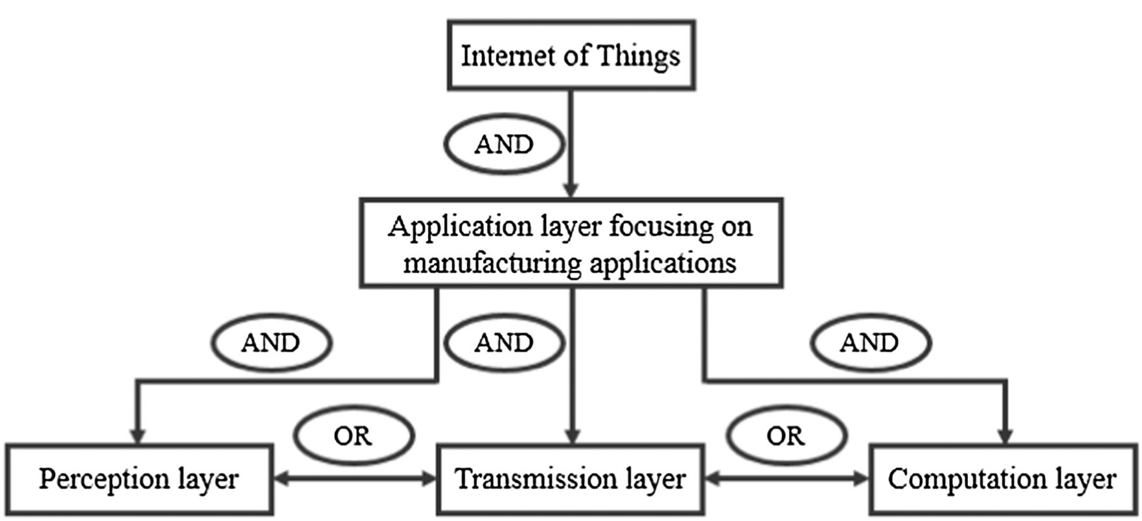

Fig. 11. Relations among search term keywords corresponding to each layer.

Please cite this article in press as: A.J.C. Trappey et al., A review of essential standards and patent landscapes for the Internet of Things: A key enabler for Industry 4.0, Adv. Eng. Informat. (2016), http://dx.doi.org/10.1016/j.aei.2016.11.007

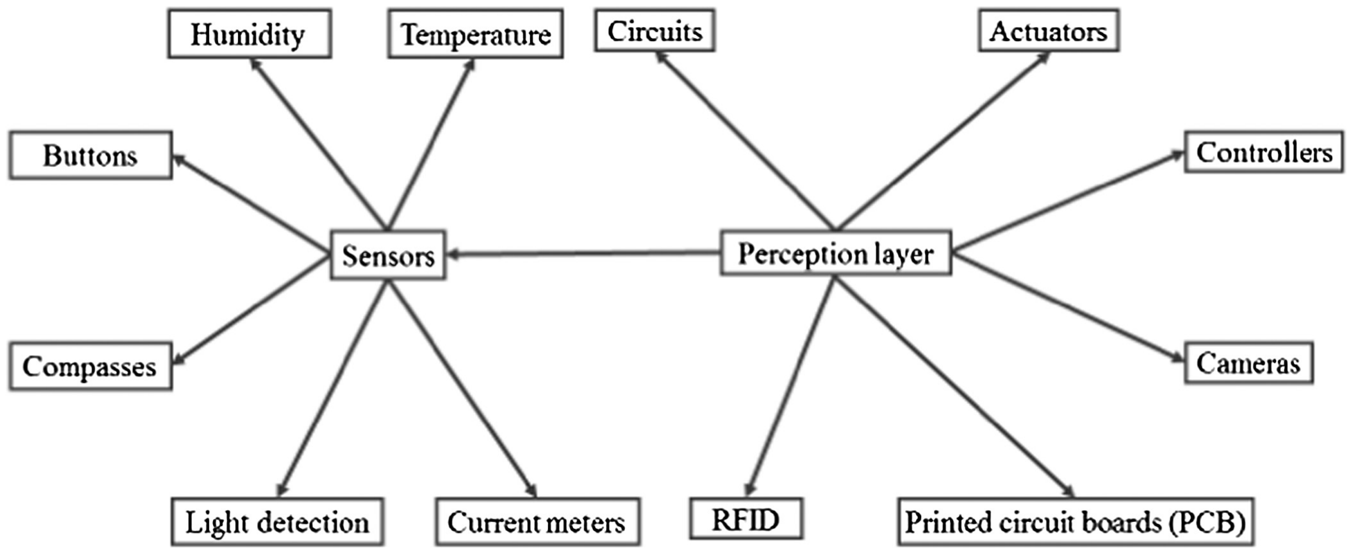

Fig. 12. Ontology for the perception layer [5,24].

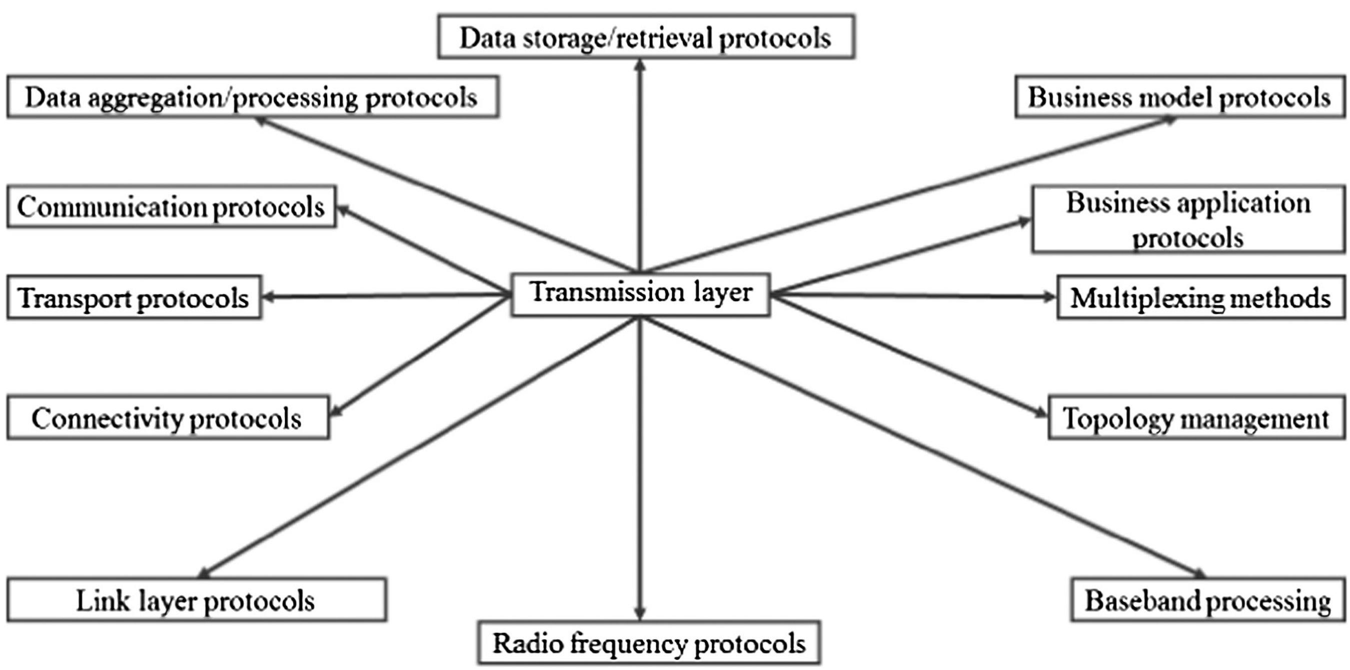

Fig. 13. Ontology for the transmission layer [9,24].

The computation layer describes the algorithms needed to create and transform the collected and transmitted data. The related technologies in the computation layer include algorithms, encryption and memory management of IoT applications, power management, resource management, IoT control systems, routing algorithms, embedded systems, cyber-physical systems, image processing, character recognition, error correction, data security, data encryption, information retrieval, localization algorithms, QoS security, intrusion detection systems, computational components, automated IoT-based access control systems, and IoT surveillance. Commercially available IoT control systems are categorized as Arduino, Beagle-Bone, Carambola 2, Dragino, Raspberry Pi, Intel Edison, Intel Grove and Nordic. Please refer to Fig. 14 for a detailed definition of the computation layer ontology [20,24].

The related technologies in the IoT application layer are defined as home, lifestyle, health, mobility, retail, energy, cities, manufacturing and public services. This research focuses on the "manufacturing" aspect of IoT applications. Please refer to Fig. 15 for detailed definitions for the application layer ontology [5,21].

5. Patent landscape analysis

In the section, the overall patent landscape analyses for the perception, transmission, computation and application layer including top assignees - IoT key players, IoT patents top IPCs and the technology application matrix are introduced.

5.1. Top assignees - IoT key players

Referring to Table 1, the top assignees are Intel, IBM, Samsung, Huawei, ZTE, Qualcomm, Ericsson, Fujitsu, Siemens, and Nokia. The leader is Intel with 133 patents followed by IBM

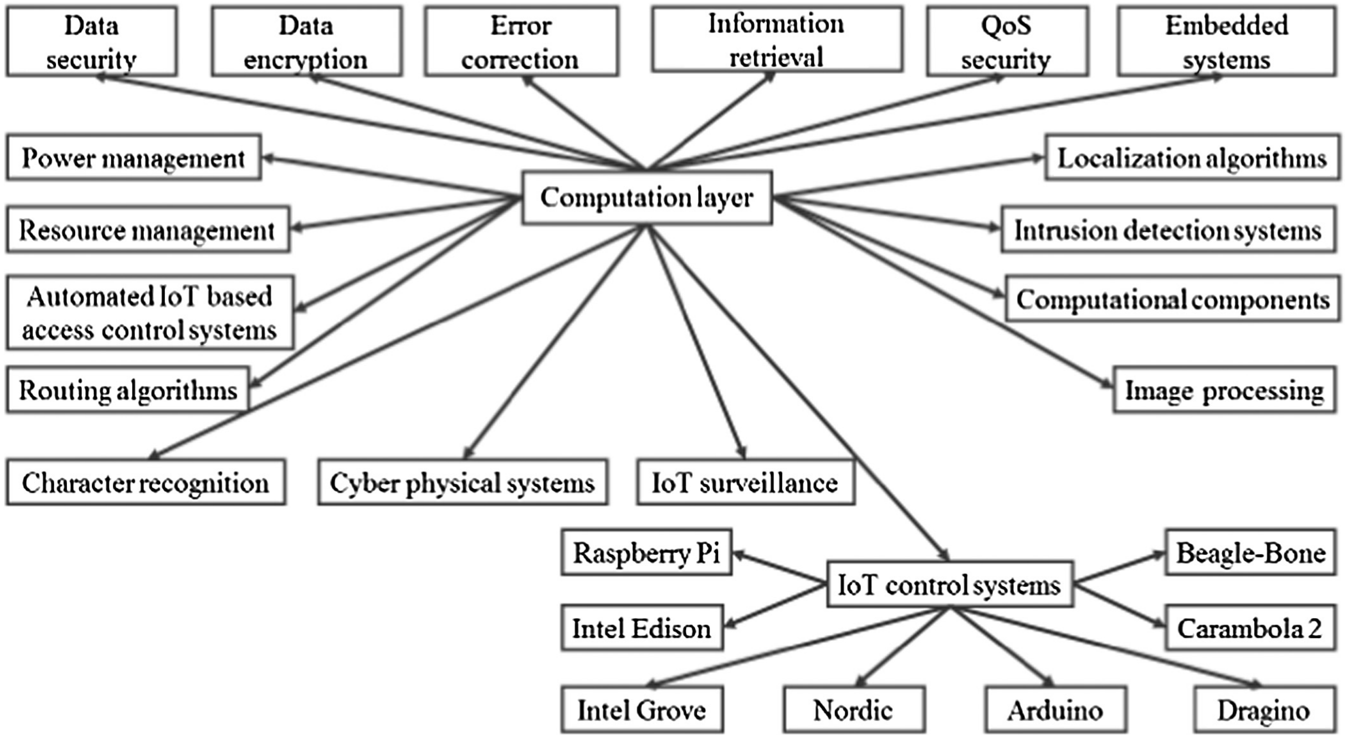

Fig. 14. Ontology for the computation layer [20,24].

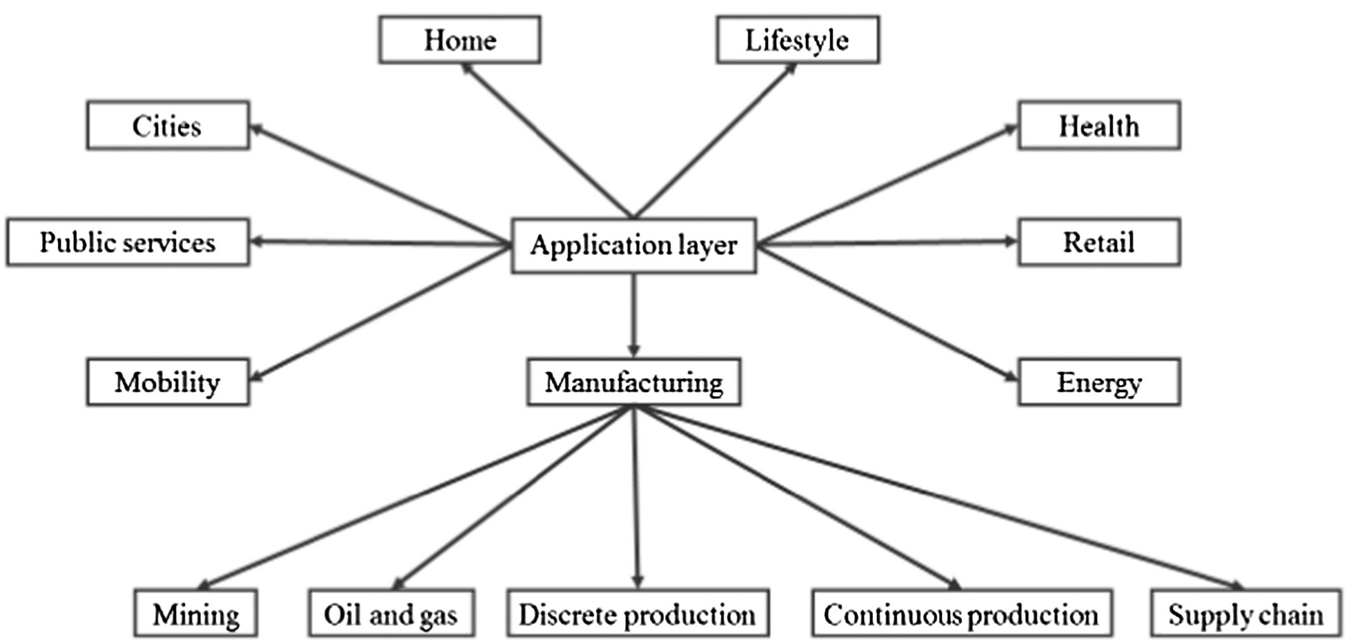

Fig. 15. Ontology for the application layer [5,21].

with 132 patents. Third place is held by Samsung with 125 patents. Huawei and ZTE follow Samsung, the former has 84 patents, and the latter has 67 patents. In the near future, Intel will focus more on the development of IoT, cloud data centers and 5th generation mobile networks which will likely enter the market in 2020 [101]. IBM cooperates with SAP to offer complementary product and service mixes including solutions to cloud computing, analysis of customer experiences, and integration services. IBM is leading the drive for customer's digital transformation, providing preemptive opportunities in the IoT market [102]. In 2015, Samsung spent about fourteen billion US dollars on the research and development of IoT, which makes the company a leader in R&D expenditures. Table 1 provides detailed information about the top assignees.

In Table 2, the largest number of patents were filed in the United States, where there are 964 patents. China has the second largest collection of related patents with Japan in third place. The total number of patents in the United States, China, Japan, and Korea represents over 80% coverage indicating these countries are the most competitive in product development for the IoT

Table 1
Top assignees rankings.

Ranking	Top assignees	Patent count
1	Intel Corp./USA	133
2	IBM/USA	132
3	Samsung Electronics CO, LTD/Korea	125
4	Huawei Tech CO, LTD/China	84
5	ZTE Corp/China	67
6	Qualcomm Inc./USA	63
7	Ericsson, Telefon AB LM/Sweden	61
8	Fujitsu LTD/Japan	59
9	Siemens A.G./Germany	48
10	Nokia Corp./Finland	47

Table 2
Top countries by assignee rankings.

Ranking	Country code	Patent count	Percentage
1	US	964	30
2	CN	721	22
3	JP	588	18
4	WO	584	18
5	KR	414	12

market. Table 2 provides detailed information about the top countries by assignee.

The US is top ranked country where the most IoT patents are filed and indicates a leading position in technology innovation and market coverage.

5.2. IoT patents' top IPCs

Table 3 describes the leading International Patent Classification (IPC) analysis. The H04L class dominates the industry with the sub-classes H04L002906 (technology focus: characterized by a protocol), H04L002908 (technology focus: Transmission control procedure, e.g. data link level control procedure) and H04L001228 (technology focus: characterized by path configuration). LAN (Local Area Networks) or WAN (Wide Area Networks). The G06F001516 sub-class (technology focus: Combinations of two or more digital computers each having at least an arithmetic unit, a program unit and a register for a simultaneous processing of several programs) belong to the G06F class and is ranked seventh with 300 patents. Most patents are classified in the H04L002906 sub-class, with a technology focus on protocols. Table 3 provides information about the top ten IPCs and their patent counts. Table 4 shows the top twenty IPCs, their ranks, and patent counts with respect to the IoT layers and sub-technologies corresponding to the IPC. The technology focus of the G05B0019418 sub-class in the application layer relates to the manufacturing control systems, such as Direct Numerical Controls (DNC), Flexible Manufacturing Systems (FMS), Integrated Manufacturing Systems (IMS) and Computer-Integrated Manufacturing (CIM), which function as essential parts in IoT. These manufacturing control systems are utilized in the manufacturing environments, in which IoT can integrate all the manufacturing machines into an inter-connective system. FMS and CIM systems can integrate the logistics and supply chains to improve logistics efficiencies. These systems can be applied traditional energy resources production industries including oil, gas, and mining. The sub-technologies in the application layer put more emphases on the applications of manufacturing control systems in the energy, production, and supply chain. Both the transmission and computation layer have more IPCs than the others. Over half of the IPCs for the transmission layer patents are ranked within the top 10 IPCs.

Table 3
Top 10 IPCs rankings.

Ranking	IPC class	Patent count
1	H04L002906	2282
2	H04L002908	1221
3	H04L001228	568
4	H04L002912	367
5	H04L001224	353
6	H04L001256	338
7	G06F001516	300
8	G06F001300	218
9	H04L002902	175
10	H04L001226	170

Table 4 shows the 20 IPCs that correspond to the four layers and the sub-technologies corresponding to the IPC class. Many patents fall into the H04L002906, H04L002908, H04L001228, H04L002912, H04L001224 and H04L001256 sub-classes. Patents in the top 3 IPCs, which are H04L002906, H04L002908, and H04L001228 sub-classes, are related to multiplexing methods, baseband processing, and protocols. For the H04L002912 sub-class, the patents relate to the protocols for GSM/GPRS networks, transmitting data in packets, IPv6, intrusion systems, real-time protocol, Java implementation, radio-frequency identification (RFID) device, network device configuration information transmission, peer-to-peer networking, network flow restoration, and medium access control (MAC) addresses. In the H04L001224 sub-class, the patents are related to connection methods of monitoring devices, systems for processing task-scheduling cloud, monitor terminal, modems used in ADSL communication systems, application providing methods in mobile communication systems, communication systems for providing a fault-tolerant communication path for narrow and broadband communications, automatic wiring devices, camera module apparatus, remote data acquisition and transmission systems, network-based communication providing methods, work-unit recovery planning and scheduling systems for reconfigurable production systems, node B buffered data recovery systems for wireless communications, solar energy connector band management systems, machine frame management systems for advanced telecom computing architectures, programmable logic controller network setting methods, network access interception controlling systems, unique provisioning methods for radio frequency identification devices, and methods for creating hierarchical sensor network for enhanced monitoring of shipping packages. On the other hand, the H04L001256 sub-class has more patents related to predetermined communication protocols, radio-frequency identification (RFID) devices, network storage, industrial control systems, internet protocol version-6 (IPv6), peer-to-peer networking, GSM/GPRS networks, authenticated distance measurement, protocol redundancy routing, client-server communication, wireless LAN, the extension to message extension protocol, the arbitration circuit for scheduling, measuring wireless device, network usage and performance metrics.

Table 5 shows the companies with the largest number of patents. Samsung, IBM, Intel, Huawei, Qualcomm, ZTE, Nokia, Ericsson, Siemens, and Fujitsu are leaders. All of the top assignees have patents with an IPC code of H04L002906. The technology focus is characterized by these protocols. Companies are focusing on the technological development for the transmission of digital information since the H04L class has more patents than other classes and many IPCs are classified in the transmission layer. Table 5 provides detailed information about the top IPCs by assignee.

Table 4
Top 20 IPCs that correspond to the four layers.

Layer	IPC class	Sub technologies corresponding to the IPC	Ranking	Patent count
Perception	H04L001224	Sensors, Circuits, Actuators, Controllers, RFID, Imaging	5	353
	H04L002910	Sensors, Circuits, Actuators, Controllers	19	111
Transmission	H04L002906	Multiplexing methods, Topology management, Baseband processing, Protocols	1	2282
	H04L002908	Multiplexing methods, Topology management, Baseband processing, Protocols	2	1221
	H04L001228	Multiplexing methods, Baseband processing, Protocols	3	568
	H04L002912	Protocols	4	367
	H04L001256	Baseband processing, Protocols	6	338
	H04L002902	Protocols	9	175
	H04L001266	Multiplexing methods, Topology management, Baseband processing, Protocols	11	166
	G06F0015173	Topology management, Protocols	15	137
	H04L001270	Multiplexing methods, Topology management, Protocols	17	128
	H04L001246	Protocols	18	116
Computation	G06F001516	Hardware, Software, Algorithms, Encryption, Memory management, Power management, Resource management	7	300
	G06F001300	Hardware, Software, Algorithms, Encryption, Resource management	8	218
	H04L001226	Hardware, Software, Cloud platforms, Encryption, Memory management, Power management, Resource management	10	170
	H04L000932	Hardware, Software, Cloud platforms, Encryption, Power management, Resource management	12	164
	H04L002914	Hardware, Software, Encryption	13	163
	G06F001730	Hardware, Software, Cloud platforms, Encryption, Memory management, Power management, Resource management	14	147
	H04L000100	Hardware, Encryption	16	132
Application	G05B0019418	Energy, Production, Supply chain	19	111

Table 5
Assignees company technology matrix.

Assignee	IPC				
	H04L001224 (Perception)	H04L001228 (Transmission)	H04L002906 (Transmission)	H04L002908 (Transmission)	H04L002912 (Transmission)
Samsung	19	66	79	44	27
IBM	18	0	97	65	13
Intel	17	16	104	29	16
Huawei	11	10	63	0	9
Qualcomm	0	9	44	32	0
ZTE	15	0	46	0	0
Nokia	0	10	42	19	0
Ericsson	0	0	46	16	7
Siemens	7	0	35	17	0
Fujitsu	9	11	0	17	7
Total	96	122	556	239	79

5.3. Top IPCs for patent families held by leading IoT key players, IBM and Intel

The research discusses the top IPCs for patent families held by the two leading IoT developers, IBM and Intel. Table 6 shows that IBM holds 118 DWPI patent families with most IPCs distributed under the H04L class. The H04L002906 sub-class (technology focus: characterized by a protocol) has the largest number of patents, 86 patents. The H04L002908 sub-class (technology focus: Transmission control procedure, such as data link level control procedure) has 60 patents and ranks second. The G06F001516 sub-class (technology focus: Combinations of two or more digital computers each having at least an arithmetic unit, a program unit and a register for a simultaneous processing of several programs) under the G06F class has 27 patents and ranks third.

Table 6
Top IPCs for patent families held by IBM.

Ranking	IPC class	Patent count
1	H04L002906	86
2	H04L002908	60
3	G06F001516	27
4	G06F0015173	22
5	H04L001224	16
6	H04L001256	12
7	H04L002912	12
8	H04L000900	12
9	G06F001730	10
10	G06F001100	9

The direction of information and communication technologies (ICT) focuses on IoT technologies. IBM targets artificial intelligence (AI) and machine learning technologies. The company has developed at over 25 types of artificial intelligence technologies including image recognition, natural language identification, and application-programming interfaces (APIs). These applications have been well accepted by the financial services, healthcare, and public services [103]. The development of cloud computing technologies has allowed enterprises to collect and analyze large amounts of data using sensors and simultaneously convert the data into useful information. Traditional industries that have demand for real-time data analysis such as mining, oil drilling, and older factories often lack the computers and bandwidth for application of the technology. During June 2016, IBM cooperated with Cisco to combine the IBM's Watson IoT platform with Cisco's Edge Analytics to provide solutions for less costly data collection and analysis [104].

Table 7
Top IPCs for patent families held by Intel.

Ranking	IPC class	Patent count
1	H04L002906	76
2	H04L002908	25
3	H04L001256	22
4	G06F001516	20
5	H04L001228	15
6	G06F001300	13
7	H04L001224	11
8	H04L002912	9
9	G06F002100	8
10	G06F0015173	5

Intel is another leading IoT key player. Table 7 shows that Intel holds 99 DWPI patent families with many IPCs falling under the H04L class. The H04L002906 sub-class (technology focus: characterized by a protocol) has 76 patents. The H04L002908 sub-class (technology focus: Transmission control procedure, such as data link level control procedure) has 25 patents, and the H04L001256 sub-class (technology focus: Packet switching systems) has 22 patents.

Intel has targeted the development of self-driving car technology and has acquired the computer vision company Itseez. This trend indicates that Intel is re-positioning from a traditional PC company into a company that will focus on the development of cloud computing and intelligent IoT equipment [105]. Intel emphasizes innovative computational performance, 5G networking technologies and IoT applications. For IoT applications, Intel has introduced two processors for gateways that are modeled on the Atom architecture. This architecture includes AnyWAN™, GRX750, and 5G XWAY WAV500 Wi-Fi communication chips based on Wi-Fi 802.11ac MU-MIMO technology standards which stabilize network communications. Intel is also working with Chunghwa Telecom, and SanJet Technology, to develop networking and remote monitoring services and car connection components [106].

5.4. Technology application matrix (TAM)

A Technology Application Matrix (TAM) uses patent data mining of archived patents to identify specific patenting activities for different manufacturing applications. The keywords from patents form the corpus for selecting the most frequent keywords which in turn are used to create the TAM. The most frequent keywords include system and method, method and apparatus, Internet protocol, wireless communication, IP address, computing device, radio frequency, physical layer, and intrusion detection. These technologies, especially wireless communication, IP address, computing device, and radio frequency, are highly related to the development of IoT. Table 8 depicts the technology application matrix, which maps the patented technologies with respect to their functions and applications. TAM helps IoT developers and manufacturers define the opportunities and risks for management science based data decisions (including simulation and scenario planning) for the development of technology [107]. The technologies and applications in Table 8 are based on the sub-technologies corresponding to the IPC in Table 4. Since the patents landscape analysis for I 4.0 has a focus on IoT, the research studies the IoT applications in manufacturing. The sub-technologies correspond to the IPC application layer for energy, production, and supply chains that form the application dimension in the matrix (the bolded text indicating the higher numbers of granted patents in Table 8).

Table 8 shows technology dominance in software, circuits, hardware, sensors, and encryption. For applications related to energy and supply chain applications, the IoT technologies have fewer patents. While compared with other technologies, multiplexing, baseband processing, memory management, power management and resource management are less utilized in the fields of energy and supply chains.

Table 8
Technology application matrix (TAM).

Technology	Application		
	Energy (A1)	Production (A2)	Supply chain (A3)
Perception layer			
Sensors (T1)	30	**211**	11
Circuits (T2)	26	**404**	5
Actuators (T3)	10	43	3
Controllers (T4)	57	**890**	7
RFID (T5)	5	**104**	14
Imaging (T6)	1	27	2
Transmission layer			
Multiplexing methods (T7)	0	**139**	0
Topology management (T8)	5	**118**	1
Baseband processing (T9)	0	18	0
Protocols (T10)	8	**531**	2
Computation layer			
Hardware (T11)	10	**255**	10
Software (T12)	25	**409**	10
Algorithms (T13)	17	**126**	1
Cloud platforms (T14)	5	50	3
Encryption (T15)	22	**211**	6
Memory management (T16)	2	**131**	0
Power management (T17)	3	75	0
Resource management (T18)	3	97	0

Increased usage of IoT technology applications will impact information security. In order to solve the problems of information security, such as anti-carjacking and component theft, new algorithms are being developed [108,109]. The areas of cybersecurity, personal privacy, security encryption, security algorithms will also yield related applications. Some companies decide to maintain their intellectual property as trade secrets so there is incomplete information which technologies are not being patented [110]. Overall, given the published data, the IoT leaders are focusing on the introduction of sensors, wireless communication, and embedded systems [111].

6. Conclusions

IoT is helping companies improve customer relationships, track tools, deliver products faster, and reduce costs. Applying Moore's law, IoT sensors will become less expensive and create new business opportunities [1,112]. The key challenges for IoT are that the current many industry software systems are a legacy, closed-box system that prevents machines from communicating with each other over the new Internet protocols of IoT [113]. Standardization is essential for technology adaptation. Specialists predict that the creation of a complete Industry 4.0 standard will take at least 10 years and may discourage small and medium enterprises from upgrading their systems due to the current investment in assets [114]. While a great deal of potential exists for advancing IoT technologies in manufacturing, many manufacturers are unaware of how to capture the potential of IoT, which is enabling everyday manufacturing objects to be connected to cloud computing via wireless sensing [112]. Similarly to the IT revolution of the last 50 years, IoT is a revolution of the next decades and will find applications in all fields of technology development as illustrated in Table 8. A gap still exists between what is possible and what

Please cite this article in press as: A.J.C. Trappey et al., A review of essential standards and patent landscapes for the Internet of Things: A key enabler for Industry 4.0, Adv. Eng. Informat. (2016), http://dx.doi.org/10.1016/j.aei.2016.11.007

is needed in industrial IoT, hence additional research, development, and publications are needed. This paper provides a standards analysis section which defines the interoperability and versatility in industrial engineering. These definitions help create a relationship among terms and systems for manufacturing followed by a section for roadmaps that depict the intellectual property ecosystem for industrial IoT. In a short summary from the research discovery, the total numbers of perception and transmission standards are the two highest types among IoT standards. Further, the IP analytics discovers the majority of IoT patents are distributed under the H04L classification, which aslo represents perception and transmission orientated patents. These inferences help estimate that the IoT market will produce a wide array of new sensors, actuators, controllers, and circuits, as well as their transmission techniques in compliance with standards and forming IP ecosystems for adaptation and commercialization. This research encourages the adoption of IoT technologies by clarifying both standards and IP topics in I 4.0 context and can be used as a point of references by both academicians who would like to explore frontier research in IoT innovations and by companies that would like to provide or adopt IoT technologies.

Acknowledgement

This research is partially supported by the Ministry of Science and Technology research grant in Taiwan (MOST 104-2218-E-007-015-MY2).

Appendix A

The following are Tables A1–A4 for standards. Most of content in scope of deliverable is from the ISO and IEC standard documents.

Table A1
Perception layer standards.

Title	Scope of deliverable (*Italics indicates exact wording of standard*)	Corresponding standard of China
ISO 6346:1995, Freight containers – Coding, identification and marking [70]	The ISO 6346:1995 *provides a system for general application for the identification and presentation of information about freight containers. It also specifies an identification system with mandatory marks for visual interpretation and optional features for automatic identification and electronic data interchange and a coding system for data on container size and type*	
ISO 10374:1991, Freight containers – Automatic identification [63]	The ISO 10374:1991 *specifies a system for the automatic identification of freight containers and the electronic transfer. It specifies all necessary user requirements including a container identification system, data coding systems, description of data, performance criteria and security features*	GB/T 17894-1999, Freight containers—Automatic identification
ISO/TS 10891:2009, Freight containers – Radio frequency identification (RFID) – License plate tag [64]	The ISO/TS 10891:2009 *includes a set of requirements for container tags, which allow the transfer of information from a container to automatic processing systems by electronic means; a data coding system for container identification and permanent related information which resides within a container tag; a data coding system for the electronic transfer of both container identification and permanent related information from container tags to automatic data processing systems; the description of data to be included in container tags for transmission to automatic data processing systems; performance criteria necessary to ensure consistent and reliable operation of container tags within the international transportation community; the physical location of container tags on containers; features to inhibit malicious or unintentional alteration and/or deletion of the information content of container tags when installed on a freight container*	GB/T 26934-2011, Freight containers radio frequency identification license plate tag
ISO/IEC 15459 series, Information technology – Automatic identification and data capture techniques – Unique identification [71]	Unique identification is used in many places such as item, transport unit, returnable transport item, and grouping. The ISO/IEC 15459 consists of 6 parts: Part 1: Individual transport units; Part 2: Registration procedures; Part 3: Common rules; Part 4: Individual products and product packages; Part 5: Individual returnable transport items (RTIs); Part 6: Groupings. *The ISO/IEC 15459 series, which can include additional rules for which level of identification should be used, are often made available from the Issuing Agency*	
ISO/IEC 15963-2009, Information technology – Radio frequency identification for item management – Unique identification for RF tags [72]	The ISO/IEC 15963:2009 *describes numbering systems that are available for the identification of RF tags. All the RF tags have unique ID. It can be used for the unique ID can be used for the traceability of the integrated circuit itself for quality control in its manufacturing process, the traceability of the RF tag during its manufacturing process and along its lifetime, for the completion of the reading in a multi-antenna configuration, by the anti-*	

(*continued on next page*)

Table A1 (*continued*)

Title	Scope of deliverable (*Italics indicates exact wording of standard*)	Corresponding standard of China
	collision mechanism to inventory multiple tags in the reader's field of view, and for the traceability of the Item to which the RF tag is attached	
ISO 17363:2013 ISO 17364:2013 ISO 17365:2013 ISO 17366:2013 ISO 17367:2013, Supply chain applications of RFID [73–77]	These standards *define the technical aspects and data hierarchy of supply chain management information required in each layer of the supply chain.* These standards include Freight containers, Returnable transport items (RTIs) and returnable packaging items (RPIs), Transport units, Product packaging, and Product tagging. These standards are designed to be interoperable and non-interfering	
ISO/IEC 18000 series, Information technology – Radio frequency identification for item management [78]	The ISO/IEC 18000 series *provides the different unique frequency range for diverse RFID technologies.* It consists of 7 parts Part 1: Reference architecture and definition of parameters to be standardized; Part 2: Parameters for air interface communications below 135 kHz; Part 3: Parameters for air interface communications at 13,56 MHz; Part 4: Parameters for air interface communications at 2,45 GHz; Part 6: Parameters for air interface communications at 860 MHz to 960 MHz; Part 7: Parameters for active air interface communications at 433 MHz. ISO/IEC 18000 series describes the different frequencies to help us utilize the different physical behaviors	
ISO 18185 series, Freight containers – Electronic seals [65]	The ISO 18185 series *create a standard for wireless data communication for e-seals and* consists of 6 parts. Part 1: Communication protocol; Part 2: Application requirements; Part 3: Environmental characteristics; Part 4: Data protection; Part 5: Physical layer	GB/T 23678-2009, Application specification of container electronic seal for supply chain monitoring
ISO/IEC 19762:2016, Information technology – Automatic identification and data capture (AIDC) techniques – Harmonized vocabulary [66]	The ISO/IEC19762:2016 *provides terms and definitions for automatic identification techniques and data entry fields are based on which other specialized sections in various technical fields, and the essential terms that must be employed by non-technical users to communicate with specialists in automatic identification and data capture techniques*	GB/T 29261 series, Information technology—Automatic identification and data capture (AIDC) techniques—Vocabulary
ISO/IEC 20005:2013, Information technology- Sensor networks- Services and interfaces supporting collaborative information processing in intelligent sensor networks [67]	The ISO/IEC 20005:2013 *specifies services and interfaces supporting collaborative information processing (CIP) in intelligent sensor networks which includes: CIP functionalities and CIP functional model, common services supporting CIP, common service interfaces to CIP*	GB/T 30269.401-2015, Information technology - Sensor networks - Part 401: Collaborative information processing: Services and interfaces supporting collaborative information processing
ISO/IEC/IEEE 21450:2010, Information technology – Smart transducer interface for sensors and actuators – Common functions, communication protocols, and Transducer Electronic Data Sheet (TEDS) formats [68]	The ISO/IEC/IEEE 21450:2010 *defines the functions that are to be performed by a transducer interface module (TIM) and the common characteristics for all devices that implement the TIM. It specifies the formats for Transducer Electronic Data Sheets (TEDS) and also defines a set of commands to facilitate the setup and control of the TIM as well as reading and writing the data used by the system. Application programming interfaces (APIs) are defined to facilitate communications with the TIM and with applications*	
ISO/IEC/IEEE 21451 series, Information technology – Smart transducer interface for sensors and actuators [69]	Part 1: Network Capable Application Processor (NCAP) information model that *defines an object model with a network-neutral interface for connecting processors to communication networks, sensors, and actuators* Part 2: Transducer to microprocessor communication protocols and Transducer Electronic Data Sheet (TEDS) formats that *defines a digital interface for connecting transducers to microprocessors. It describes a Transducer Electronic Data Sheet (TEDS) and its data formats. It defines an electrical interface, read and write logic functions to access the TEDS, and a wide variety of transducers* Part 4: Mixed-mode communication protocols and Transducer Electronic Data Sheet (TEDS) formats that *define the protocol and interface that allows analog transducers to communicate digital information with an ISO/IEC/IEEE 21451 object. It also defines the format of the Transducer Electronic Data Sheet (TEDS), which is based on the ISO/IEC/IEEE 21451-2 TEDS* Part 7: Transducer to radio frequency identification (RFID) systems communication protocols and Transducer Electronic Data Sheet (TEDS) format	

Please cite this article in press as: A.J.C. Trappey et al., A review of essential standards and patent landscapes for the Internet of Things: A key enabler for Industry 4.0, Adv. Eng. Informat. (2016), http://dx.doi.org/10.1016/j.aei.2016.11.007

Table A1 (*continued*)

Title	Scope of deliverable (*Italics indicates exact wording of standard*)	Corresponding standard of China
	Part 7 defines data formats to facilitate communications between radio frequency identification (RFID) systems and smart RFID tags with integral transducers (sensors and actuators). It defines new Transducer Electronic Data Sheet (TEDS) formats based on the ISO/IEC/IEEE 21451 series of standards. It also defines a command structure and specifies the communication methods with which the command structure is designed to be compatible	
ISO/IEC 29143:2011, Information technology – Automatic identification and data capture techniques – Air interface specification for Mobile RFID interrogators [80]	The ISO/IEC 29143:2011 *provides an air interface specification for Mobile radio frequency identification (RFID) interrogators being part of a passive backscatter system. The interface specifies mobile RFID interrogator media access control, interrogator to interrogator and multiple interrogator to tag collision arbitration scheme including interrogator requirements, interrogator to interrogator and multiple interrogator to tag collision avoidance scheme, and tag memory use for Mobile RFID applications*	
ISO/IEC TR 29172:2011 ISO/IEC 29173-1:2012 ISO/IEC 29175 :2012 ISO/IEC 29176 :2011 ISO/IEC 29178 :2012 ISO/IEC 29179:2012, Information technology – Mobile item identification and management [81–86]	The series of standards are used to *define Mobile AIDC services*. These standards *include reference architecture for Mobile AIDC services, Mobile RFID interrogator device protocol, User data for Mobile AIDC services, Consumer privacy-protection protocol for Mobile RFID services, Service broker for Mobile AIDC services, and Mobile AIDC application programming interface*	
ISO/IEC 29182 series, Sensor networks: Sensor Network Reference Architecture (SNRA) [61]	The ISO/IEC 29182 series contains seven sections and *provides the guidance for designing and developing the sensor networks. The purpose is to increase interoperability of sensor networks, and make sensor network components run smoothly. The ISO/IEC 29182 series focuses on a generic architecture for sensor networks. It can be used by sensor network designers, software developers, system integrators, and service providers*	
ISO/IEC 30101:2014, Information technology – Sensor networks: Sensor network and its interfaces for smart grid system [88]	The ISO/IEC 30101:2014 *is for sensor networks in order to support smart grid technologies for power generation, distribution, networks, energy storage, load efficiency, control and communications, and associated environmental challenges. It describes the interfaces between the sensor networks and other networks; Sensor network architecture to support smart grid systems; Interface between sensor networks with smart grid systems; Sensor network based emerging applications and services to support smart grid systems*	
ISO/IEC 30128:2014, Information technology – Sensor networks – Generic Sensor Network Application Interface [89]	The ISO/IEC 30128:2014 *specifies the interfaces between the application layers of service providers and sensor network gateways. It Describes Generic sensor network applications' operational requirements; Sensor network capabilities; Mandatory and optional interfaces between the application layers of service providers and sensor network gateways*	

Table A2
Transmission layer standards.

Title	Scope of deliverable	Corresponding standard of China
ISO/IEC 8802 series, Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks [62]	The ISO/IEC 8802 includes many parts, such as ISO/IEC TR 8802-1:2001, ISO/IEC 8802-2:1998, ISO/IEC/IEEE 8802-3:2014, ISO/IEC/IEEE 8802-3-1:2015, ISO/IEC 8802-5:1998, ISO/IEC/IEEE 8802-11:2012, ISO/IEC/IEEE 8802-22:2015, and ISO/IEC/IEEE 8802-15-4:2010. *It provides an introduction to the set of International Standards which describe local area networks*	GB/T 15629 series, Information technology—Local and metropolitan area networks
ISO/IEC 14476 series, Information technology – Enhanced communications transport protocol [60]	The ISO/IEC 14476 series is used to enhance communications transport protocol. It consists of 6 parts. Part 1: simplex multicast transport, Part 2: QoS management for simplex multicast transport, Part 3: duplex multicast transport, Part 4: QoS management	GB/T 26241 series, Information technology - Enhanced communication transport protocol

(*continued on next page*)

Table A2 (*continued*)

Title	Scope of deliverable	Corresponding standard of China
	for duplex multicast transport, Part 5: N-plex multicast transport, and Part 6: QoS management for n-plex multicast transport	
IEC 61158 series, Industrial communication networks – Fieldbus specifications [53]	The IEC 61158 series is the fieldbus standard. IEC 61158 series consists of 6 parts. Part 1: Overview and guidance for the IEC 61158 and IEC 61784 series, Part 2: Physical Layer specification and service definition, Part 3: Data Link Service definition, Part 4: Data Link Protocol specification, Part 5: Application Layer Service definition, Part 6: Application Layer Protocol specification. These standards are formulated for real-time distributed control and composed of many industrial computer network protocols	GB/T 19582, GB/T 19760, GB/T 20171, GB/T 20540, GB/Z 20541, GB/T 25105, GB/Z 26157, GB/T 27960, GB/Z 29619, GB/T 29910, GB/T 31230
EC 61784 series, Industrial communication networks - Profiles [54]	The IEC 61784 series is the profiles standard of fieldbus. IEC 61784 consists of 5 parts. Part 1: Fieldbus profiles, Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3, Part 3: Functional safety fieldbuses, Part 4: Security, and Part 5: Installation of fieldbuses. IEC 61784 series *defines a set of protocol specific communication profiles based primarily on the IEC 61158 series. It can be used in the design of devices involved in communications in factory manufacturing and process control*	
IEC 62591:2016, Industrial networks – Wireless communication network and communication profiles - Wireless HART™ [58]	IEC 62591:2016 *defines a wireless communication network, including physical layer service definition and protocol specification, data-link layer service and protocol, application layer service and protocol, network management, security, communication profile, wireless procedures and gateway*	GB/T 29910.5-2013, Industrial communication networks - Fieldbus specifications - Type 20 HART specification - Part 5:WirelessHART wireless communication network and communication profile
IEC 62601:2015, Industrial networks - Wireless communication network and communication profiles - WIA-PA [59]	IEC 62601 *defines the system architecture and the communication protocol of Wireless networks for Industrial Automation - Process Automation (WIA-PA). WIA-PA system architecture and communication protocol are discussed in this standard, and suitable for industrial measurement and monitoring of wireless network system*	GB/T 26790 series, Industrial wireless networks WIA specification

Table A3
Computation layer standards.

Title	Scope of deliverable	Corresponding standard of China
ISO/IEC 27033 series, Information technology – Security techniques – Network security [79]	The ISO/IEC 27033 series is to *provide detailed guidance on the security aspects of the management, operation and use of information system networks, and their interconnections. Those individuals within an organization that are responsible for information security in general, and network security in particular, should be able to adapt the material in ISO/IEC 27033 series to meet their specific requirements.* ISO/IEC 27033 series consists of 6 parts. Part 1: Overview and concepts. Part 2: Guidelines for the design and implementation of network security. Part 3: Reference networking scenarios – Threats, design techniques and control issues. Part 4: Securing communications between networks using security gateways Part 5: Securing communications across networks using Virtual Private Networks (VPNs) Part 6: Securing wireless IP network access	
ISO/IEC 29180: 2012, Information technology – Telecommunications and information exchange between systems – Security framework for ubiquitous sensor networks [87]	The ISO/IEC 29180:2012 *describes the security threats to and security requirements of the ubiquitous sensor network (USN). In addition, it categorizes the security technologies according to the security functions that satisfy the said security requirements and where the security technologies are applied in the security model of the USN*	
IEC 62443 series (ISA99), Security for Industrial Automation and Control Systems [56]	IEC62443 series of standards divided into 4 parts general, information security program, system technology and component technologies. IEC62443 series of standards used these 4 parts to achieve comprehensive security protection. *The primary goal of the IEC 62443 series is to provide a flexible framework*	GB/T 30976.1-2014, Industrial control system security—Part 1:Assessment specification GB/T 30976.2-2014, Industrial control system security—Part 2:Acceptance specification

Table A3 (*continued*)

Title	Scope of deliverable	Corresponding standard of China
	that facilitates addressing current and future vulnerabilities in Automation and Control Systems and applying necessary mitigations in a systematic, defensible manner. IEC 62443 series is to build extensions to enterprise security that adapt the requirements for business IT systems and combines them with the unique requirements for strong availability needed by Automation and Control Systems	

Table A4
Application layer standards.

Title	Scope of deliverable	Corresponding standard of China
IEC 61804-3, IEC 61804-4, IEC 61804-5, IEC 61804-6 Function blocks (FB) for process control - Electronic device description language (EDDL) [55]	These four parts of IEC 61804 series define the EDDL. EDDL is a language that can be used to describe the characteristics of devices. Device suppliers can use EDDL to create Electronic Device Description (EDD) files instead of using XML	GB/T 21099-3-2010, Function block (FB) for process control—Part 3: Electronic device description language (EDDL) GB/T 21099-4-2010, Function block (FB) for process control - Part 4:EDD interoperability guideline
IEC 62453 - Field device tool (FDT) interface specification [56]	IEC 62453 introduces the concept of FDT as well as the definition of the relevant terms about FDT. *FDT is used for standardization of communication and configuration interfaces between all field equipment and host systems. This standard is applicable to all kinds of industrial applications, such as engineering system, monitoring and diagnostic applications*	GB/T 29618 series, Field device tool (FDT) interface specification

Appendix B

See Table B1.

Table B1
Keywords for each layer of IoT.

Perception layer	Transmission layer	Computation layer	Application layer
• Circuits • Sensors – Temperature – Open/Closed – Accelerometer Tilt – Voltage Detect – Dry Contact – Impact Detect – Carbon Monoxide – G-force Snapshot – Pressure Meter – Light Detection – G-force Max & Avg – Light Meter – Current Meter – Button – Asset – Compass – Water Detect – Input Pulse Counter – Resistance – Flex – Voltage Meter – Air Flow Detection – Humidity – Activity Detection – Liquid Level – Grains Per Pound – Activity Vibration Counting – Vehicle Detection – Motion Detection – Activity Timer – Vehicle Counter	• Multiplexing Methods • Topology Management • Baseband Processing • Radio Frequency Protocols • Internet Protocol (IP) • Network Protocol • Medium Access Control Protocol • Wireless Sensor • Network • Connectivity Protocols – Mocbus – ODB2 – PLC – RJ45 – RS-232 – RS-485 – SPI – USB – Wireless • Link Layer Protocols – BLE – Bluetooth – CDMA – Dash 7 – Ethernet 802.3 – GSM – Wifi 802.11 a/b/g/n – Zigbee – 802.15.4e • Transport Protocols – IPv4 – IPv6 – 6LoWPAN	• Power Management • Resource Management • IoT Control System – Arduino – Beagle-Bone – Carambola 2 – Dragino – Raspberry Pi – Intel Edison – Intel Grove – Nordic • Cyber-Physical System • Embedded System • Automated IoT Based Access Control System • Software – IDE – OS – Database • Algorithms – Routing Algorithm – Localization Algorithm – Image Processing – Character Recognition • Cloud Platform – Hadoop – Nimbits • Encryption – Error Correction – Data Security – Data Encryption – QoS Security – Intrusion Detection System – IoT Surveillance	• Home – Home Automation – Home Improvement – Energy Efficiency • Lifestyle – Wearable Computing – Entertainment – Family – Leisure – Pets – Toys – Drones • Health – Fitness – Monitoring – Measurement – Diagnosis – Monitoring – Measurement – Diagnosis – Surgery – Patient Care • Mobility – Connected Cars – eBikes – Aerospace & Airports – Marine – Rail &Stations – Automotive – Traffic • Retail – Stores – Shops

(*continued on next page*)

Table B1 (*continued*)

Perception layer	Transmission layer	Computation layer	Application layer
– Image • Actuators • Controllers • RFID technology • Printed Circuit Board (PCB) • Camera	– RPL • Session/Communication Protocols – AMQP – CoAP – DDS – FTP – HTTP – MQTT – SSH – Telnet – XMPP • Data Aggregation/Processing Protocols – Fluentd – Flume – Kafka – RapidMQ – Scribe – Storm • Data Storage/Retrieval Protocols – Cassandra – Hadoop – HBase – MongoDB • Business Model Protocols – Closed – Cloud – Direct – Indirect – Integrated – On demand – On Premise – Open – Platform • Business Application Protocols – Device Management – Business Processes – Analytics	• Memory Management – Information Retrieval • Computational Component	– Convenience • Energy – Transmission & Distribution – Fossil – Nuclear – Alternative • Cities – Infrastructure – Water/Wastewater – HVAC – Lighting – Security – Life Safety • Manufacturing – Mining – Oil & Gas – Discrete Production – Continuous Production – Supply Chain • Public Services – Schools – Universities – Government – Banking – Insurance – Administration – Commercial Services • Others – Environment – Military – Agriculture – Hospitality

References

[1] F.T. Cheng, H. Tieng, H.C. Yang, M.H. Hung, Y.C. Lin, C.F. Wei, Z.Y. Shieh, Industry 4.1 for wheel machining automation, IEEE Robot. Autom. Lett. 1 (1) (2016) 332–339.

[2] H. Kagermann, J. Helbig, A. Hellinger, W. Wahlster, Securing the Future of German Manufacturing Industry: Recommendations for Implementing the Strategic Initiative Industrie 4.0, ACATECH, 2013.

[3] Pocket-lint, Internet of Things Explained: What is it, and can it really change the World? <http://www.pocket-lint.com/news/126559-internet-of-things-explained-what-is-it-and-can-it-really-change-the-world> (last accessed: 05/05/2016).

[4] M.U. Farooq, M. Waseem, S. Mazhar, A. Khairi, T. Kamal, A review on Internet of Things (IoT), Int. J. Comput. Appl. 113 (1) (2015) 1–7.

[5] Z. Yang, Y. Peng, Y. Yue, X. Wang, Y. Yang, W. Liu, Study and application on the architecture and key technologies for IOT, in: International Conference on Multimedia Technology (ICMT), IEEE, 2011, pp. 747–751.

[6] M. Wu, T.L. Lu, F.Y. Ling, L. Sun, H.Y. Du, Research on the architecture of Internet of things, 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), vol. 5, 2010, pp. 484–487.

[7] N. Elgendy, A. Elragal, Big data analytics: a literature review paper, in: Advances in Data Mining. Applications and Theoretical Aspects, Springer International Publishing, 2014, pp. 214–227.

[8] H.S. Bhosale, D.P. Gadekar, A review paper on big data and hadoop, Int. J. Sci. Res. Publ. 4 (10) (2014) 756–764.

[9] Blog post by Antony, The Internet of Things Protocol Stack – From Sensors to Business Value, 2014. <https://entrepreneurshiptalk.wordpress.com/2014/01/29/the-internet-of-thing-protocol-stack-from-sensors-to-business-value/> (last accessed: 03/31/2016).

[10] Deutschlands Zukunft als Produktionsstandort, sichernUmsetzungsempfehlungen für das ZukunftsprojektIndustrie 4.0, 2013. <https://www.bmbf.de/files/Umsetzungsempfehlungen_Industrie4_0.pdf> (last accessed: 05/03/2016).

[11] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of Things (IoT): a vision, architectural elements, and future directions, Future Gener. Comput. Syst. 29 (7) (2013) 1645–1660.

[12] S. Krco, B. Pokric, F. Carrez, Designing IoT architecture(s): a European perspective, in: Proc. IEEE WF-IoT, 2014, pp. 79–84.

[13] M. Gerla, L. Eun-Kyu, G. Pau, L. Uichin, Internet of vehicles: from intelligent grid to autonomous cars and vehicular clouds, in: Proc. IEEE WF-IoT, 2014, pp. 241–246.

[14] I. Ungurean, N.C. Gaitan, V.G. Gaitan, An IoT architecture for things from industrial environment, in: Proc. 10th Int. COMM, 2014, pp. 1–4.

[15] C. Wang, Z. Bi, L.D. Xu, IoT and cloud computing in automation of assembly modeling systems, IEEE Trans. Ind. Inform. 10 (2) (2014) 1426–1434.

[16] Github, IoT Code Recipes: RPL, mDNS and REST, 2016. <http://github.com/mehdimo/IoTCodeRecipes> (last accessed: 05/1/2016).

[17] B.B. Olyaei, J. Pirskanen, O. Raeesi, A. Hazmi, M. Valkama, Performance comparison between slotted IEEE 802.15.4 and IEEE 802.1 lah in IoT based applications, in: Proc. IEEE 9th Int. Conf. WiMob, 2013, pp. 332–337.

[18] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, Internet of things: a survey on enabling technologies, protocols, and applications, Commun. Surv. Tutor., IEEE 17 (4) (2015) 2347–2376.

[19] S. Hachem, T. Teixeira, V. Issarny, Ontologies for the Internet of Things, in: Proceedings of the 8th Middleware Doctoral Symposium, 2011, pp. 3:1–3:6.

[20] F. Xia, L.T. Yang, L. Wang, A. Vinel, Internet of things, Int. J. Commun. Syst. 25 (9) (2012) 1101–1102.

[21] H. Kopetz, Internet of Things, In Real-Time Systems, Springer, US, 2011, pp. 307–323.

[22] J. Song, S. Han, A.K. Mok, D. Chen, M. Lucas, M. Nixon, WirelessHART: applying wireless technology in real-time industrial process control, in: Real-Time and Embedded Technology and Applications Symposium. RTAS'08, IEEE, 2008, pp. 377–386.

[23] S. Madakam, R. Ramaswamy, S. Tripathi, Internet of Things (IoT): a literature review, J. Comput. Commun. 3 (5) (2015) 164–173.

[24] LexInnova, Internet of Things (IoT) Patent Landscape Analysis, 2015. <http://www.lex-innova.com/resources-reports/?id=33> (last accessed: 04/10/2016).

[25] Standardization Administration of Industry and Information Technology, the National Intelligent Manufacturing System Standards Guide, 2015.

[26] IERC, Internet of Things Position Paper on Standardization for IoT technologies EUROPEAN RESEARCH CLUSTER ON THE INTERNET OF THINGS, 2015. <http://www.internet-of-things-research.eu/pdf/IERC_Position_Paper_IoT_Standardization_Final.pdf> (last accessed: 04/20/2016).

[27] IEC, About IEC, 2016 <http://www.iec.ch/about/> (last accessed: 04/10/2016).

[28] ISO, About ISO, 2016 <http://www.iso.org/iso/home/contact_iso.htm/> (last accessed: 04/10/2016).

Please cite this article in press as: A.J.C. Trappey et al., A review of essential standards and patent landscapes for the Internet of Things: A key enabler for Industry 4.0, Adv. Eng. Informat. (2016), http://dx.doi.org/10.1016/j.aei.2016.11.007

[29] Sangkeun YOO, Convenor, ISO/IEC JTC 1/WG 10 Working Group on Internet of Things, 2015. <http://iot-week.eu/wp-content/uploads/2015/06/07-JTC-1-WG-10-Introduction.pdf> (last accessed: 04/20/2016).
[30] IEC, ISO/IEC JTC 1 Scope, 2016. <http://www.iec.ch/dyn/www/f?p=103:7:0::::FSP_ORG_ID,FSP_LANG_ID:3387,25?q=jtc1%20sc%2038> (last accessed: 04/10/2016).
[31] GB/T 15629 Series: Information Technology—Local and Metropolitan area Networks.
[32] GB/T 19582 Series: Modbus Industrial Automation Network Specification.
[33] GB/T 19760 Series: CC-Link (Control & Communication Link) Specification.
[34] GB/T 20171: EPA System Architecture and Communication Specification for use in Industrial Control and Measurement Systems, 2006.
[35] GB/T 20540 Series: Digital Data Communication for Measurement and Control—Fieldbus for use in Industrial Control Systems.
[36] GB/T 21099 Series: Function Block (FB) for Process Control.
[37] GB/T 25105 Series: Industrial Communication Networks—Fieldbus Specifications—Type 10: PROFINET IO Specifications.
[38] GB/T 26241 Series: Information Technology - Enhenced Communication Transport Protocol.
[39] GB/T 26790 Series: Industrial Wireless Networks WIA Specification.
[40] GB/T 27960 Series: Ethernet POWLINK Communication Profile Specification, 2011.
[41] GB/T 29618 Series: Field Device Tool (FDT) Interface Specification.
[42] GB/T 29910 Series: Industrial Communication Networks - Fieldbus Specifications - Type 20 HART Specification.
[43] GB/T 30269-401: Information Technology - Sensor Networks - Part 401: Collaborative Information Processing: Services and Interfaces Supporting Collaborative Information Processing, 2015.
[44] GB/T 31230 Series: Industrial Ethernet Fieldbus EtherCAT.
[45] GB/Z 20541 Series: Digital Data Communication for Measurement and Control—Fieldbus for use in Industrial Control Systems—Type 10: PROFINET Specification.
[46] GB/Z 26157 Series: Digital Data Communication for Measurement and Control—Fieldbus for use in Industrial Control Systems—Type 2: ControlNet and EtherNet/IP Specification.
[47] GB/Z 29619 Series: Digital Data Communication for Measurement and Control—Fieldbus for use in Industrial Control Systems—Type 8: INTERBUS Specification.
[48] GB/T 17894: Freight Containers—Automatic Identification, 1999.
[49] GB/T 26934: Freight Containers Radio Frequency Identification License Plate Tag, 2011.
[50] GB/T 23678: Application Specification of Container Electronic Seal for Supply Chain Monitoring, 2009.
[51] GB/T 29261 Series: Information Technology—Automatic Identification and Data Capture (AIDC) Techniques—Vocabulary.
[52] GB/T 30976 Series: Industrial Control System Security.
[53] IEC 61158 Series: Industrial Communication Networks - Fieldbus Specifications.
[54] IEC 61784 Series: Industrial Communication Networks - Profiles.
[55] IEC 61804-3, IEC 61804-4, IEC 61804-5, IEC 61804-6 Function Blocks (FB) for Process Control - Electronic Device Description Language (EDDL).
[56] IEC 62443 Series (ISA99): Security for Industrial Automation and Control Systems.
[57] IEC 62453 Series: Field Device Tool (FDT) Interface Specification.
[58] IEC 62591: Industrial Networks - Wireless Communication Network and Communication Profiles - WirelessHART™, 2016.
[59] IEC 62601: Industrial Networks - Wireless Communication Network and Communication Profiles - WIA-PA, 2015.
[60] ISO/IEC 14476 Series: Information Technology – Enhanced Communications Transport Protocol.
[61] ISO/IEC 29182 Series: Information Technology – Sensor Networks: Sensor Network Reference Architecture (SNRA).
[62] ISO/IEC 8802 series: Information Technology – Telecommunications and Information Exchange between Systems – Local and Metropolitan Area Networks – Specific Requirements.
[63] ISO 10374: Freight Containers – Automatic Identification, 1991.
[64] ISO/TS 10891: Freight Containers – Radio Frequency Identification (RFID) – License Plate Tag, 2009.
[65] ISO 18185 Series, Freight Containers – Electronic Seals.
[66] ISO/IEC 19762: Information Technology – Automatic Identification and Data Capture (AIDC) Techniques – Harmonized Vocabulary, 2016.
[67] ISO/IEC 20005: Information Technology- Sensor Networks- Services and Interfaces Supporting Collaborative Information Processing in Intelligent Sensor Networks, 2013.
[68] ISO/IEC/IEEE 21450: Information Technology – Smart Transducer Interface for Sensors and Actuators – Common Functions, Communication Protocols, and Transducer Electronic Data Sheet (TEDS) Formats, 2010.
[69] ISO/IEC/IEEE 21451 Series: Information Technology – Smart Transducer Interface for Sensors and Actuators.
[70] ISO 6346: Freight Containers – Coding, Identification and Marking, 1995.
[71] ISO/IEC 15459 Series: Information Technology – Automatic Identification and Data Capture Techniques – Unique Identification.
[72] ISO/IEC 15963: Information Technology – Radio Frequency Identification for Item Management – Unique Identification for RF Tags, 2009.
[73] ISO 17363: Supply Chain Applications of RFID-Freight Containers.
[74] ISO 17364: Supply Chain Applications of RFID- Returnable Transport Items (RTIs) and Returnable Packaging Items (RPIs).
[75] ISO 17365: Supply Chain Applications of RFID-Transport Units.
[76] ISO 17366: Supply Chain Applications of RFID-Product Packaging.
[77] ISO 17367: Supply Chain Applications of RFID - Product Tagging.
[78] ISO/IEC 18000 Series: Information Technology – Radio Frequency Identification for Item Management.
[79] ISO/IEC 27033 Series: Information Technology – Security Techniques – Network Security.
[80] ISO/IEC 29143: Information Technology – Automatic Identification and Data Capture Techniques – Air Interface Specification for Mobile RFID Interrogators, 2011.
[81] ISO/IEC TR 29172: Information Technology – Mobile Item Identification and Management -Reference Architecture for Mobile AIDC Services, 2011.
[82] ISO/IEC 29173-1: Information Technology – Mobile Item Identification and Management – Part 1: Mobile RFID Interrogator Device Protocol for ISO/IEC 18000-63 Type C, 2012.
[83] ISO/IEC 29175: Information Technology – Mobile Item Identification and Management – User Data for Mobile AIDC Services, 2012.
[84] ISO/IEC 29176: Information Technology – Mobile Item Identification and Management – Consumer Privacy-protection Protocol for Mobile RFID Services, 2011.
[85] ISO/IEC 29178: Information Technology — Mobile Item Identification and Management — Service Broker for Mobile AIDC Services, 2012.
[86] ISO/IEC 29179: Information Technology – Mobile Item Identification and Management – Mobile AIDC Application Programming Interface, 2012.
[87] ISO/IEC 29180: Information Technology — Telecommunications and Information Exchange between Systems — Security Framework for Ubiquitous Sensor Networks, 2012.
[88] ISO/IEC 30101: Information Technology – Sensor Networks: Sensor Network and its Interfaces for Smart Grid System, 2014.
[89] ISO/IEC 30128: Information Technology – Sensor Networks – Generic Sensor Network Application Interface, 2014.
[90] ISO/IEC JTC 1, Internet of Things (IoT), 2015.
[91] DIN, German Standardization Roadmap – Industry 4.0 (Version 2), DIN e. V., Berlin, January 2016. Available: <http://www.din.de/blob/65354/f5252239daa596d8c4d1f24b40e4486d/roadmap-i4-0-e-data.pdf> (last accessed: 09/21/2016).
[92] S.B. Jhu, C.P. Wei, C.C. Du, Research and prospect for the application of internet of things in sensing and safety, China Saf. Sci. J. 20 (11) (2010) 164–170.
[93] FDT Group, FDT Technology, what is it, 2016. <http://www.fdtgroup.org/fdt-technology-what-it> (last accessed: 04/10/2016).
[94] DeltaV Whitepaper, Why Electronic Device Description Language (EDDL) Technology is the Right Choice for Smart Plant Installations, 2013. <http://www2.emersonprocess.com/siteadmincenter/PM%20DeltaV%20Documents/Whitepapers/WP_EDDL.pdf> (last accessed: 04/27/2016).
[95] IEC TC3/TC65, IoT Relevant Standardization in IEC TC3 and IEC TC65, 2014. <https://www.google.com.tw/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjQzYDK057KAhVkIaYKHS8vCSkQFggcMAA&url=http%3A%2F%2Fec.europa.eu%2FDocsRoom%2Fdocuments%2F5114%2Fattachments%2F1%2Ftranslations%2Fen%2Frenditions%2Fnative&usg=AFQjCNGf2KRa6pH_y_h3vbAJtDEOy_qgOQ&sig2=mHM6drceWXRmUkTj4QU1Dw> (last accessed: 09/20/2016).
[96] Finnegan, Standard-Essential Patents and Pooling, 2015. <http://www.finnegan.com/files/upload/Newsletters/IP_Marketplace/2015/October/IPM_Resources_Oct15.pdf> (last accessed: 04/10/2016).
[97] UK Intellectual Property Office Informatics Team, Eight Great Technologies - The Internet of Things - A Patent Overview, 2014. <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/343879/informatics-internet.pdf> (last accessed: 09/21/2016).
[98] WIPO, PCT – The International Patent System, 2015. <http://www.wipo.int/pct/en/faqs/faqs.html> (last accessed: 09/10/2016).
[99] MBA lib, International Application of a Patent, 2015. <http://wiki.mbalib.com/zh-tw/%E4%B8%93%E5%88%A9%E5%9B%BD%E9%99%85%E7%94%B3%E8%AF%B7> (last accessed: 09/15/2016).
[100] Intellogist, French Patent Office (INPI) Website, 2009. <http://www.intellogist.com/wiki/French_Patent_Office_(INPI)_Website> (last accessed: 09/15/2016).
[101] UDN News, Intel focuses on cloud data centers and IoT, 2016. <http://udn.com/news/story/7087/1656349-Intel> (last accessed: 05/04/2016).
[102] IBM, IBM and SAP Announce Plans for Major Investments to Drive Clients' Digital Transformations, 2016. <http://www-03.ibm.com/press/us/en/pressrelease/49458.wss> (last accessed: 04/10/2016).
[103] UDN News, Six technologies spotlight... Business Opportunities Appear, 2016. <http://udn.com/news/story/7240/1755872-%E5%85%AD%E6%8A%80%E8%A1%93%E8%81%9A%E5%85%89%E2%80%A6%E5%95%86%E6%A9%9F%E7%88%86%E7%99%BC> (last accessed: 06/12/2016).
[104] iThome, Cisco Routers will be Integrated with IBM's Waston IoT, and Strengthen the Ability to the Boundary Network Equipment Analysis, 2016. <http://www.ithome.com.tw/news/106379> (last accessed: 06/03/2016).
[105] Xfastest, Intel Acquires a Computer Vision Company to enter the Internet of Things and Self-driving Cars, 2016. <https://news.xfastest.com/intel/20586/%E8%8B%B1%E7%89%B9%E7%88%BE%E6%94%B6%E8%B3%BC%E8%A8%88%E7%AE%97%E8%A6%96%E8%A6%BA%E5%85%AC%E5%8F%B8%EF%BC%8C%E9%80%B2%

Please cite this article in press as: A.J.C. Trappey et al., A review of essential standards and patent landscapes for the Internet of Things: A key enabler for Industry 4.0, Adv. Eng. Informat. (2016), http://dx.doi.org/10.1016/j.aei.2016.11.007

E8%BB%8D%E7%89%A9%E8%81%AF%E7%B6%B2%E8%88%87%E7%84%A1%E4%BA%BA%E9%A7%95%E9%A7%9B/> (last accessed: 06/03/2016).

[106] UDN News, Intel Creates Gateways and Networking Chips to Expand Internet of things, 2016. <http://udn.com/news/story/7091/1731087-%E6%93%B4%E5%A4%A7%E7%89%A9%E8%81%AF%E7%B6%B2-Intel%E6%89%93%E9%80%A0%E9%96%98%E9%81%93%E5%99%A8%E3%80%81%E9%80%A3%E7%B6%B2%E6%99%B6%E7%89%87> (last accessed: 06/03/2016).

[107] T.Y. Cheng, A new method of creating technology/function matrix for systematic innovation without expert, J. Technol. Manage. Innovat. 7 (1) (2012) 118–127.

[108] TechNews, Microsoft Announced Seven Major Digital Crime Trends, and Asia has become a Horror-level Battlefield, 2014. <http://technews.tw/2014/11/27/microsoft-announces-global-7-digital-crime-trends-in-asia-has-become-a-horror-level-armies/> (last accessed: 09/19/2016).

[109] EE Times Taiwan, Hackers will become the Hidden Problems for Automobiles in the Future, 2015. <http://archive.eettaiwan.com/www.eettaiwan.com/ART_8800714490_675327_NT_d6c0ae63.HTM#.Vb97bpOqpYI> (last accessed: 09/19/2016).

[110] ADLINK Tech, Machine-failure-prediction, 2016. <http://www.adlinktech.com/big5/Internet_of_Things/Machine-Failure-Prediction.php?utm_source> (last accessed: 09/19/2016).

[111] Digitimes, Establishment of Industrial Internet of Things (IIoT) for the Upcoming Industry 4.0 era, 2016. <http://www.digitimes.com.tw/tw/iot/shwnws.asp?cnlid=15&id=0000472361_X04289YU7NIU9C0YF8GMP&ct=1> (last accessed: 09/19/2016).

[112] An NSF Workshop Report, NSF Workshop on Advanced Manufacturing for Smart Goods, Brian k. Paul, Oregon State University, May 14–15, 2015.

[113] E.-A. Lee, Cyber-physical systems-are computing foundations adequate, in: Position Paper for NSF Workshop on Cyber-Physical Systems: Research Motivation, Techniques and Roadmap, vol. 2, October 2006.

[114] APROS - Services and Consulting, Industry 4.0 Globally Networked – Controlled as if by Magic, Customer Magazine of Rehm Thermal Systems, 2014. Available: <http://news.blog.apros-consulting.de/globally-networked-controlled-as-if-by-magic-industry-4-0/> (accessed on April 20, 2016).

Please cite this article in press as: A.J.C. Trappey et al., A review of essential standards and patent landscapes for the Internet of Things: A key enabler for Industry 4.0, Adv. Eng. Informat. (2016), http://dx.doi.org/10.1016/j.aei.2016.11.007